



Complexité de la résolution des systèmes algébriques paramétriques.

Ali Ayad

► To cite this version:

Ali Ayad. Complexité de la résolution des systèmes algébriques paramétriques.. Mathématiques [math]. Université Rennes 1, 2006. Français. NNT: . tel-00127383

HAL Id: tel-00127383

<https://theses.hal.science/tel-00127383>

Submitted on 29 Jan 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

N° d'ordre : 3410

THÈSE

présentée

DEVANT L'UNIVERSITÉ DE RENNES 1

pour obtenir

le grade de : **DOCTEUR DE L'UNIVERSITÉ
DE RENNES 1**

Mention Mathématiques et Applications

par

Ali AYAD

Institut de Recherche Mathématique de Rennes

École Doctorale MATISSE

U.F.R. de Mathématiques

TITRE DE LA THÈSE :

**Complexité de résolution de systèmes
algébriques paramétrés.**

Soutenue le 13 Octobre 2006 devant la commission d'examen

COMPOSITION DU JURY :

M.	Dimitry	GRIGORYEV	Directeur
M.	Pascal	KOIRAN	Rapporteur
M.	Bernard	MOURRAIN	Rapporteur
M.	Fabrice	ROUILLIER	Examineur
Mme.	Marie-Françoise	ROY	Examinatrice
M.	Eric	SCHOST	Examineur

Complexité de résolution de systèmes algébriques paramétrés

Mai 2006

Remerciements

Je tiens à remercier avant tout mon directeur de thèse Dimitry Grigoryev, pour m'avoir guidé avec patience tout au long de ces trois années et pour m'avoir permis de mener à bien cette thèse.

Merci à Pascal Koiran et à Bernard Mourrain d'avoir accepté d'être rapporteurs.

Merci à Fabrice Rouillier, Marie-Françoise Roy et Eric Schost d'avoir accepté de faire partie du jury.

Merci également à tous les membres de mon équipe de travail et à toute personne qui m'a écouté tout au long de cette période.

Merci aussi aux secrétaires et aux bibliothécaires de l'IRMAR qui ont toute ma gratitude pour leur efficacité et pour leur gentillesse.

Merci à Peter Bürgisser et à son groupe pour les aides et les discussions qu'on a eu pendant mon séjour à Paderborn en Allemagne en 2005.

Enfin, un grand merci à ma famille et à mes amis qui m'ont supporté et qui m'ont encouragé tout au long de cette thèse.

Table des matières

1	Etat de l'art	6
1.1	Introduction	7
1.1.1	Notations	7
1.1.2	Résolution	8
1.2	Historique et Algorithmes	11
1.2.1	Résolution de systèmes linéaires paramétrés	11
1.2.2	Calcul d'un P.G.C.D. d'une famille finie de polynômes univariés paramétrés	11
1.2.3	Résolution de systèmes algébriques paramétrés	12
1.3	Nos contributions principales	16
1.3.1	Modèle de calcul	16
1.3.2	Résolution de systèmes paramétrés zéro-dimensionnels	17
1.3.3	Factorisation absolue des polynômes paramétriques	19
1.3.4	Résolution de systèmes paramétrés de dimensions positives	20
2	Quelques algorithmes intermédiaires	25
2.1	Factorisation de polynômes sans paramètres	26
2.1.1	Factorisation sur le corps des nombres rationnels	26
2.1.2	Factorisation sur un corps fini	26
2.1.3	Factorisation sur une extension algébrique	27
2.1.4	Factorisation absolue	27
2.2	Résolution de systèmes algébriques sans paramètres	29
2.2.1	Historique	29
2.2.2	Algorithme de Chistov-Grigoriev	34
2.3	Elimination de quantificateurs dans la théorie des corps algébriquement clos	40
2.3.1	Description du problème	40
2.3.2	Historique	42
2.3.3	Algorithme de Chistov-Grigoriev	44
2.4	Résolution des systèmes linéaires paramétriques	45
2.4.1	Algorithme de Gauss paramétrique	46
2.5	Calcul d'un P.G.C.D. d'une famille finie de polynômes univariés paramétrés	49
2.5.1	Algorithme A1	50
2.5.2	Algorithme A2	53

2.5.3	Algorithme A3	54
3	Résolution de systèmes algébriques paramétrés de dimensions zéros	56
3.1	Introduction et notations	57
3.2	Résultant paramétrique	58
3.3	U-Résultant paramétrique	60
3.4	Vecteur constant des multiplicités	64
3.5	Shape lemma paramétrique	67
4	Factorisation absolue des polynômes paramétrés	74
4.1	Introduction et notations	75
4.2	Préparation au lemme de Hensel	76
4.3	Lemme de Hensel	82
4.4	Partition de l'espace des paramètres par le lemme de Hensel	87
4.5	Théorème principal	92
4.6	Cas général	96
5	Résolution de systèmes algébriques paramétrés de dimensions positives	98
5.1	Introduction et notations	99
5.2	Arbres des composantes	99
5.3	Base de l'induction	103
5.4	Hypothèses de l'induction	108
5.5	Coeur de l'induction	110
5.5.1	Construction de h_{m+1}	111
5.5.2	Réduction au cas paramétrique zéro-dimensionnel	112
5.5.3	Construction d'un point générique efficace paramétrique de chaque composante $W_{w_m}^{(a)}$	116
5.5.4	Construction d'un système représentatif paramétrique de chaque composante $W_{w_m}^{(a)}$	119
5.6	Analyse de la complexité totale de l'algorithme du théorème 5.2.5	121
5.7	Description des composantes des variétés $V^{(a)}$	122
6	Appendice	123
6.1	Notions de complexité	124
6.1.1	Complexité binaire	124
6.1.2	Symboles de complexité	124
6.1.3	Complexité d'évaluation des polynômes multivariés	125
6.2	Algèbre linéaire	125
6.3	Théorie combinatoire	126
6.3.1	Partitions des entiers	126
6.3.2	Principe de Dirichlet	126
6.4	Variétés projectives	127
6.4.1	Dimension	128

6.4.2	Degré	130
-------	-----------------	-----

Chapitre 1

Etat de l'art

1.1 Introduction

Un système algébrique polynomial est un ensemble fini de polynômes multivariés à coefficients dans un corps F . Résoudre un tel système revient à trouver les zéros communs de ses polynômes dans une clôture algébrique \overline{F} de F .

La question posée est de décrire l'ensemble de solutions de ce système en distinguant deux cas possibles :

- Si cet ensemble est fini (i.e., le système est zéro-dimensionnel), celle-là revient à donner ces solutions explicitement.
- Si cet ensemble est infini (i.e., le système est de dimension positive), une façon de le décrire est d'exprimer les variables du système comme de fonctions de quelques paramètres qui peuvent être pris parmi ces variables.

La résolution des systèmes algébriques est l'un des problèmes importants de la géométrie algébrique et du calcul formel. La simulation de plusieurs phénomènes physiques [85, 107, 44], chimiques [41, 44, 54], optimisation [122], interpolation [109, 110, 54], robots [55, 31, 109, 110] et des problèmes géométriques [47, 83] conduit à des systèmes d'équations polynomiales à paramètres. Un système algébrique paramétrique est une collection infinie de systèmes algébriques paramétrisés par un nombre fini de variables appelées les paramètres du système.

1.1.1 Notations

Considérons une famille (f_1, \dots, f_k) de polynômes dans $F[u, X]$ paramétrisés par les variables $u = (u_1, \dots, u_r)$ (les paramètres), homogènes en les variables $X = (X_0, \dots, X_n)$ de degré d chacun. Ces polynômes définissent un système polynomial paramétré $f_1 = \dots = f_k = 0$, l'ensemble $\mathcal{P} = \overline{F}^r$ sera appelé l'espace des paramètres. Pour tout point $a = (a_1, \dots, a_r) \in \mathcal{P}$ (spécialisation des paramètres), on note par $V^{(a)}$ la variété projective de $P^n(\overline{F})$ définie par les polynômes homogènes $f_1^{(a)}, \dots, f_k^{(a)} \in \overline{F}[X_0, \dots, X_n]$, où

$$f_i^{(a)} = f_i(a_1, \dots, a_r, X_0, \dots, X_n), 1 \leq i \leq k$$

D'une manière générale, pour un polynôme $g \in F(u_1, \dots, u_r)[X_0, X_1, \dots, X_n]$, on note par $g^{(a)}$ le polynôme de $\overline{F}[X_0, X_1, \dots, X_n]$ obtenu en remplaçant u_1, \dots, u_r par a_1, \dots, a_r respectivement dans g lorsque les dénominateurs des coefficients de g ne s'annulent pas en a .

Exemple 1.1.1 *Considérons le système paramétré suivant qui décrit l'état d'un bras ar-*

ticulé constitué de deux tiges de longueur 1 [55, 109, 110] :

$$\begin{cases} x_1 + x_2 = u \\ x_3 + x_4 = v \\ x_1^2 + x_3^2 = 1 \\ x_2^2 + x_4^2 = 1 \end{cases}$$

Les variables u et v sont les paramètres, les inconnues sont les variables x_1, \dots, x_4 .

1.1.2 Résolution

Pour un tel système algébrique paramétré (f_1, \dots, f_k) , on peut poser la question suivante : Qu'est-ce qu'une résolution ?

La réponse à cette question dépend du problème original qui a donné naissance à ce système. Par exemple on se demande parfois de trouver les valeurs des paramètres là où le système spécialisé (i.e., le système obtenu après spécialisation des paramètres) admet une solution, i.e., trouver le lieu de consistance du système dans l'espace des paramètres. Ceci est équivalent à calculer l'ensemble $\mathcal{U}_1 = \{a \in \mathcal{P}, V^{(a)} \neq \emptyset\}$ qui n'est autre que la \overline{F} -réalisation dans la théorie des corps algébriquement clos de la formule suivante :

$$(\exists X_0) \cdots (\exists X_n) f_1(u_1, \dots, u_r, X_0, \dots, X_n) = \cdots = f_k(u_1, \dots, u_r, X_0, \dots, X_n) = 0$$

cette formule admet u_1, \dots, u_r comme variables libres. Le calcul de \mathcal{U}_1 revient donc à éliminer les quantificateurs de cette formule, ce qui sera étudié dans le chapitre 2.

Parfois on se demande de calculer l'ensemble $\mathcal{U}_2 \subset \mathcal{U}_1 \subset \mathcal{P}$ formé par les valeurs des paramètres $a \in \mathcal{U}_1$ tel que la variété $V^{(a)}$ est un sous-ensemble fini de $P^n(\overline{F})$, i.e., le système $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ est zéro-dimensionnel. Ou bien de décrire les sous-ensembles $\mathcal{U}_{2,s}$ de \mathcal{U}_2 là où le système associé admet exactement s solutions distinctes dans $P^n(\overline{F})$, i.e., $\mathcal{U}_{2,s} := \{a \in \mathcal{U}_2, \sharp(V^{(a)}) = s\}$ pour tout $1 \leq s \leq d^n$. Par conséquence, calculer les solutions de ce système d'une façon uniforme sur les paramètres, i.e., décrire une représentation paramétrique des solutions comme de fonctions rationnelles paramétrées des racines d'un polynôme univarié paramétré [109, 110], ce qu'on appelle une résolution géométrique paramétrique du système (voir le paragraphe suivant et le chapitre 3). Celle-ci est donnée dans l'exemple suivant :

Exemple 1.1.2 Reprenons l'exemple précédent, une résolution géométrique paramétrique de ce système est donnée par [109, 110] :

$$x_4^2 - vx_4 + \frac{1}{4} \frac{u^4 + 2u^2v^2 - 4u^2 + v^4}{u^2 + v^2} = 0, \quad \begin{cases} x_1 = \frac{v}{u}x_4 + \frac{1}{2} \frac{u^2 - v^2}{u^2 + v^2} \\ x_2 = -\frac{v}{u}x_4 + \frac{1}{2} \frac{u^2 + v^2}{u} \\ x_3 = -x_4 + v \end{cases}$$

Soit le sous-ensemble constructible U_1 de l'espace des paramètres \mathbb{C}^2 défini par les inéquations suivantes :

$$u \neq 0, \quad u^2 + v^2 \neq 0$$

Pour toute spécialisation (a, b) des paramètres (u, v) dans U_1 les solutions $(x_1, \dots, x_4) \in \mathbb{C}^4$ du système correspondant sont obtenues par extraction des racines (i.e., x_4) d'une équation du second degré à coefficients dans \mathbb{C} . Les valeurs de (x_1, x_2, x_3) sont données en fonction de ces racines.

Dans le cas général, peut-on décomposer l'espace des paramètres \mathcal{P} en un nombre fini d'ensembles constructibles \mathcal{U} deux à deux disjoints tel que pour chaque \mathcal{U} le nombre des composantes absolument irréductibles de la variété associé est constant, i.e., pour tout $a, b \in \mathcal{U}$ les deux variétés projectives $V^{(a)}$ et $V^{(b)}$ ont le même nombre des composantes absolument irréductibles qui est borné par le nombre de Bézout d^n [66, 125, 15, 112]. En plus décrire chacune de ces composantes W par l'intermédiaire de deux voies suivantes :

a) Calculer un point générique *efficace* de W [125, 22, 23, 101]. Ceci est équivalent à calculer des polynômes $\phi, B_0, \dots, B_n \in F(C, u)(t_1, \dots, t_{n-m})[Z]$ et $\chi \in F(u)[C]$ où $m = \text{codim}(W)$, t_1, \dots, t_{n-m} sont de variables algébriquement indépendantes sur \overline{F} et C, Z sont de nouvelles variables et à calculer un indice s , $0 \leq s \leq n$ et une puissance p^ν où p est le caractéristique de F (p^ν est supposé égale à 1 si F est de caractéristique zéro). Pour tout $a \in \mathcal{U}$, il existe une racine c de $\chi^{(a)}$ dans \overline{F} qui vérifie :

- Les coefficients rationnels de ϕ, B_0, \dots, B_n (resp. χ) sont bien définis en (c, a) (resp. a).

- La composante W n'est pas contenue dans l'hyperplan $V(X_s) \subset P^n(\overline{F})$.

- Les fractions $\left(\frac{X_0}{X_s}\right)^{p^\nu}, \dots, \left(\frac{X_n}{X_s}\right)^{p^\nu}$ sont des fonctions rationnelles sur W définies par

$$\phi^{(c,a)}(\theta) = 0, \quad \begin{cases} \left(\frac{X_0}{X_s}\right)^{p^\nu} = B_0^{(c,a)}(\theta) \\ \vdots \\ \left(\frac{X_n}{X_s}\right)^{p^\nu} = B_n^{(c,a)}(\theta) \end{cases}$$

où θ est algébrique sur le corps $\overline{F}(t_1, \dots, t_{n-m})$ de polynôme minimal diviseur de $\phi^{(c,a)} \in \overline{F}(t_1, \dots, t_{n-m})[Z]$.

Ceci nous donne une résolution géométrique paramétrique au sens de [47, 52] pour chaque composante, i.e., une représentation paramétrique des éléments de toutes les composantes par une spécialisation des paramètres par des valeurs dans \mathcal{U} .

b) Calculer une famille finie de polynômes homogènes $\psi_1, \dots, \psi_M \in F(C, u)[X_0, \dots, X_n]$.

Pour tout $a \in \mathcal{U}$, il existe une racine c de $\chi^{(a)}$ dans \overline{F} qui vérifie :

- Les coefficients rationnels de ψ_1, \dots, ψ_M sont bien définis en (c, a) .
- Les polynômes homogènes $\psi_1^{(c,a)}, \dots, \psi_M^{(c,a)} \in \overline{F}[X_0, \dots, X_n]$ définissent la composante W , i.e.,

$$W = V(\psi_1^{(c,a)}, \dots, \psi_M^{(c,a)}) \subset P^n(\overline{F}).$$

Exemple 1.1.3 Reprenons encore une fois l'exemple précédent, on se demande que se passe-t-il pour des valeurs (a, b) des paramètres dans $\mathbb{C}^2 \setminus U_1$, i.e., $a = 0$ ou $a^2 + b^2 = 0$?.

En effet, on peut décomposer \mathbb{C}^2 en 4 ensembles constructibles U_1, \dots, U_4 donnés par les équations et les inéquations qui les définissent ainsi pour chacun d'eux on donne une représentation paramétrique des solutions valable pour toute spécialisation des paramètres dans cet ensemble. Plus précisément,

$$U_1 = \{u \neq 0, u^2 + v^2 \neq 0\}, \quad \theta^2 - \frac{-u^4 + 4u^2 - u^2v^2}{u^2 + v^2} = 0, \quad \begin{cases} x_1 = \frac{v}{2u}\theta + \frac{u}{2} \\ x_2 = -\frac{v}{2u}\theta + \frac{u}{2} \\ x_3 = -\frac{1}{2}\theta + \frac{3v}{2} \\ x_4 = \frac{1}{2}\theta + \frac{v}{2} \end{cases}$$

$$U_2 = \{u \neq 0, u^2 + v^2 = 0\}, \quad \text{pas de solutions.}$$

$$U_3 = \{u = 0, v \neq 0\}, \quad \theta^2 + \frac{v^2}{4} - 1 = 0, \quad \begin{cases} x_1 = \theta \\ x_2 = -\theta \\ x_3 = \frac{v}{2} \\ x_4 = \frac{v}{2} \end{cases}$$

$$U_4 = \{(0, 0)\}, \quad \theta^2 + t^2 - 1 = 0, \quad \begin{cases} x_1 = \theta \\ x_2 = -\theta \\ x_3 = -t \\ x_4 = t \end{cases}$$

On remarque que le système est zéro-dimensionnel sur U_1, U_2, U_3 et de dimension 1 sur U_4 (t est un paramètre qui prend des valeurs dans \mathbb{C}).

Dans cette thèse nous considérons le cas général en décrivant un algorithme qui donne une telle partition de l'espace des paramètres et en étudiant sa complexité (voir le dernier paragraphe de ce chapitre et le chapitre 5 pour plus des détails). D'abord nous décrivons quelques algorithmes de la littérature pour résoudre des systèmes polynomiaux paramétrés avec leurs bornes de complexité dans le paragraphe suivant et ensuite nous montrons nos algorithmes dans le dernier paragraphe. Il faut signaler que personne n'a étudié la décomposition de variétés paramétrées en composantes irréductibles avant notre contribution.

1.2 Historique et Algorithmes

Nous montrons dans cette section quelques algorithmes de résolution de systèmes algébriques avec paramètres.

1.2.1 Résolution de systèmes linéaires paramétrés

Considérons le cas d'un système paramétré d'équations linéaires (i.e. chaque f_i , $1 \leq i \leq k$ est une forme linéaire en $X = (X_0, \dots, X_n)$ à coefficients dans $F[u_1, \dots, u_r]$). Plus généralement, les systèmes linéaires paramétrés avec second membre ont été étudiés par Heintz en 1983 [66]. Sa méthode est basée sur une version paramétrique de l'algorithme d'élimination de Gauss et elle est utilisée pour décrire un algorithme d'élimination de quantificateurs dans la théorie des corps algébriquement clos. Un autre algorithme présenté par W. Sit [113, 114] qui décompose le lieu de consistance (i.e., l'ensemble U_1 défini ci-dessus) en un nombre fini de sous-ensembles S (appelés régimes du système). Pour chaque S , cet algorithme calcule une matrice Z de dimension $n \times (\nu + 1)$ à coefficients des fonctions rationnelles de $F(u)$ avec colonnes Z_0, Z_1, \dots, Z_ν qui vérifient les propriétés suivantes :

- a) Les entrées de Z sont bien définies sur S , i.e., pour tout $a \in S$, les dénominateurs de ces entrées ne s'annulent pas en a .
- b) Pour tout $a \in S$, $Z_0^{(a)} \in V^{(a)}$ (i.e., $Z_0^{(a)}$ est une solution particulière du système spécialisé par a) et la famille $\{Z_1^{(a)}, \dots, Z_\nu^{(a)}\}$ forme une base du système homogène associé.

1.2.2 Calcul d'un P.G.C.D. d'une famille finie de polynômes univariés paramétrés

Pour $n = 1$, Grigoriev [59] a décrit un algorithme de résolution d'un système paramétrique d'équations polynomiales univariées par la construction d'un plus grand commun diviseur d'une famille des polynômes univariés à coefficients paramétriques. De même, dans [8], chapitre 1, on trouve un algorithme de même nature que celui de Grigoriev [59], basé sur une version paramétrique de l'algorithme d'Euclide. Ces algorithmes décomposent l'espace des paramètres \mathcal{P} en de sous-ensembles constructibles W deux à deux disjoints. Pour chaque ensemble W , l'algorithme calcule un polynôme paramétrique $g \in F[u_1, \dots, u_r][X_1]$ qui constitue un témoin du P.G.C.D de la famille des polynômes $f_1, \dots, f_k \in F[u_1, \dots, u_r][X_1]$, i.e., pour toute spécialisation des paramètres $a \in W$, le polynôme $g^{(a)} \in \overline{F}[X_1]$ est un P.G.C.D de $f_1^{(a)}, \dots, f_k^{(a)} \in \overline{F}[X_1]$. Donc pour tout $a \in W$, $V^{(a)} = V(g^{(a)}) \subset \overline{F}$, i.e. $V^{(a)}$ coïncide avec l'ensemble des racines du polynôme $g^{(a)} = g(a, X_1) \in \overline{F}[X_1]$ dans \overline{F} . La complexité de l'algorithme de [59] est polynomiale en k, d et exponentielle en r tandis que celle de [8] est exponentielle en k, d et

r (voir le chapitre 2 pour plus de détails et pour d'autres algorithmes pour ce problème).

1.2.3 Résolution de systèmes algébriques paramétrés

Nous décomposons ce paragraphe en deux parties : la première partie traite les algorithmes et les méthodes existants qui calculent l'ensemble \mathcal{U}_2 défini ci-dessus en le partageant en un nombre fini d'ensembles constructibles et en décrivant les solutions (en nombre fini) du système correspondant par une représentation paramétrique. La deuxième partie considère le cas général.

1- Cas dimension zéro :

Plusieurs algorithmes sont destinés à la résolution de systèmes algébriques paramétrés zéro-dimensionnels. Parmi les outils et les techniques utilisés on distingue l'opérateur de Newton-Hensel [109, 110, 65], le calcul d'une base de Gröbner paramétrique [60, 100], les ensembles triangulaires paramétriques [33, 111] et les variétés discriminantes [84]. Dans ce paragraphe on décrit les entrées et les sorties de ces algorithmes, leurs représentations, les conditions sur le système d'entrée ainsi que leurs complexités.

1-a- Résolution géométrique paramétrique [109, 110, 65] :

On se place dans le cas où $f_1, \dots, f_k \in F[u_1, \dots, u_r, X_1, \dots, X_n]$ et $k = n$, soit $K = F(u) = F(u_1, \dots, u_r)$ le corps des fonctions rationnelles en les paramètres à coefficients dans F . Considérons l'idéal $I = \langle f_1, \dots, f_n \rangle \subset F[u_1, \dots, u_r, X_1, \dots, X_n]$, $J = I : \text{jac}((f_1, \dots, f_n), X)^\infty$ est la saturation de I par le Jacobien déterminant de (f_1, \dots, f_n) et J_K est l'extension de J dans $K[X_1, \dots, X_n]$.

Une résolution géométrique paramétrique du système (f_1, \dots, f_n) est une description des solutions simples du système de la manière suivante :

$$\phi(\theta) = 0, \quad \begin{cases} x_1 = B_1(\theta) \\ \vdots \\ x_n = B_n(\theta) \end{cases}$$

où $\theta = \sum_{1 \leq i \leq n} \alpha_i x_i$ est un élément primitif de l'extension finie $K \subset K[X_1, \dots, X_n]/J_K$, les polynômes $\phi, B_1, \dots, B_n \in K[Z]$, les degrés de leurs coefficients par rapport aux paramètres sont bornés par d^n .

Dans sa thèse Schost [109, 110] a décrit un algorithme probabiliste qui calcule une résolution géométrique paramétrique du système (f_1, \dots, f_n) avec une complexité $d^{O(rn)}$ simplement exponentielle en le nombre d'inconnues du système. Cet algorithme calcule aussi l'équation d'une hypersurface S de l'espace des paramètres là où la spécialisation échoue, i.e., $\forall a \in \mathcal{P}$, si $a \in S$ l'un de dénominateurs des coefficients de ϕ, B_1, \dots, B_n

s'annule en a et si $a \notin S$, les solutions simples du système $f_1^{(a)} = \dots = f_n^{(a)} = 0$ sont obtenues par une spécialisation des paramètres en a dans la résolution paramétrique. Le degré de cette équation est borné par $d^{O(n)}$ et la variété S est appelée une variété discriminante du système au sens de [84].

Remarquons que puisque J_K est un idéal zéro-dimensionnel de $K[X_1, \dots, X_n]$, une représentation rationnelle univarié [108, 49, 51, 2] nous donne une résolution géométrique paramétrique.

1-b- Bases de Gröbner paramétriques :

En ce qui concerne les bases de Gröbner paramétriques dans le cas zéro-dimensionnel, un algorithme est décrit dans [60] qui calcule les équations et les inéquations qui définissent l'ensemble constructible \mathcal{U}_2 défini ci-dessus. Cet algorithme partage \mathcal{U}_2 en un nombre fini d'ensembles constructibles W chacun avec une base de Gröbner paramétrique $G_1, \dots, G_m \in F(u)[X]$ qui vérifient :

- 1) Les coefficients de G_1, \dots, G_m dans $F(u)$ sont bien définis sur W .
- 2) Pour tout $a \in W$, la famille $G_1^{(a)}, \dots, G_m^{(a)}$ est une base de Gröbner réduite du système $(f_1^{(a)}, \dots, f_k^{(a)})$ (pour un ordre monomial fixé).
- 3) Le vecteur des multiplicités des solutions du système est constant sur W et il est calculé par l'algorithme.

Cet algorithme a une complexité $d^{O(rn^2)}$ simplement exponentielle en le nombre n des variables dans le cas où f_1, \dots, f_k sont donnés en représentation dense.

Dans [61] Grigoriev montre que le nombre des vecteurs des multiplicités des solutions des systèmes polynomiaux est doublement exponentiel en le nombre n des variables. Plus précisément, pour des systèmes avec $n = d$, il construit $N \geq d^{d^{\Omega(n)}}$ éléments de l'espace des paramètres distincts deux à deux et pour chacun d'eux il attribue un certain système polynomial zéro-dimensionnel avec des vecteurs des multiplicités distincts deux à deux. En particulier, le nombre des ensembles constructibles qui constituent une partition de \mathcal{P} avec les propriétés 1), 2) et 3) ci-dessus est doublement exponentiel en n , ce qui donne une borne inférieure doublement exponentielle en n de la complexité de construction d'une telle partition.

1-c- Ensembles triangulaires paramétriques[33, 111] :

Soit $V = V(f_1, \dots, f_n) \subset \overline{F}^{n+r}$ la variété affine définie par $f_1, \dots, f_n \in F[u_1, \dots, u_r, X_1, \dots, X_n]$, on suppose que la projection de V sur les r premiers va-

riables u_1, \dots, u_r est dense dans \overline{F}^r pour la topologie de Zariski. Cette condition implique que l'extension J de l'idéal $I = \langle f_1, \dots, f_n \rangle \subset F[u_1, \dots, u_r, X_1, \dots, X_n]$ dans $F(u)[X_1, \dots, X_n]$ est un idéal zéro-dimensionnel. Les zéros de J sont appelés les solutions génériques de V . Dans [33] on trouve un algorithme probabiliste qui calcule un ensemble triangulaire paramétrique $(T_1, \dots, T_n) \in F(u)[X_1, \dots, X_n]$ tel que $J = \langle T_1, \dots, T_n \rangle$, $T_i \in F(u)[X_1, \dots, X_i]$ unitaire en X_i et les degrés des coefficients de chaque T_i par rapport aux paramètres sont bornés par $2d^{2n}$ tandis que dans [111] ces degrés sont bornés par $d^{O(n^2)}$.

Cet algorithme calcule aussi une hypersurface $S \subset \overline{F}^r$ défini par un polynôme de degré $\leq d^n$ tel que $\forall a \notin S$, les dénominateurs des coefficients de T_1, \dots, T_n ne s'annulent pas en a et $V(T_1^{(a)}, \dots, T_n^{(a)}) = V(f_1^{(a)}, \dots, f_n^{(a)})$. La complexité de cet algorithme est $d^{O(nr)}$, polynomiale en la taille de sa sortie.

1-d- Variétés discriminantes [84] :

Soit π la projection de \overline{F}^{n+r} sur l'espace des paramètres $\mathcal{P} = \overline{F}^r$. Une variété discriminante du système paramétré (f_1, \dots, f_k) est une sous-variété W de \mathcal{P} tel que pour tout ouvert U de $\mathcal{P} \setminus W$, la restriction de π sur $\pi^{-1}(U) \cap V$ est un revêtement analytique de U .

La variété discriminante minimale du système (f_1, \dots, f_k) est l'intersection de toutes ses variétés discriminantes. Lazard et Rouillier [84] ont proposé un algorithme efficace du calcul de la variété discriminante minimale. Le degré de cette variété ainsi que la complexité de cet algorithme sont simplement exponentiels en le nombre n des variables.

2- Cas général :

Cette section recouvre les deux cas : zéro-dimensionnel et dimension positive.

2-a- Résolution géométrique paramétrique[47] :

Sous certaines conditions sur le système (f_1, \dots, f_k) , la clôture algébrique de Zariski $\overline{\mathcal{U}_1}$ de \mathcal{U}_1 est une hypersurface de l'espace des paramètres. Une équation polynomiale de degré minimal qui définit cette hypersurface est donnée dans [47]. Il s'agit d'appliquer la méthode de résolution géométrique de [49, 52] sur le système paramétrique (f_1, \dots, f_k) . Une description d'une solution générique du système est donnée comme une fonction rationnelle des paramètres définie sur cette hypersurface.

2-b- Bases de Gröbner paramétriques :

Les bases de Gröbner constituent un outil pratique pour résoudre des systèmes algébriques [13, 31, 38]. Elles permettent aussi de calculer la clôture algébrique de Zariski $\overline{\mathcal{U}_1}$ de \mathcal{U}_1 par une méthode d'élimination des variables X_1, \dots, X_n [31]. Pour un système

algébrique paramétré (f_1, \dots, f_k) , on procède de deux façons suivantes :

- Calculer une base de Gröbner de l'idéal engendré par f_1, \dots, f_k dans $F(u_1, \dots, u_r)[X_1, \dots, X_n]$ en respectant un certain ordre monomial sur les monômes en X_1, \dots, X_n .
- Calculer une base de Gröbner de l'idéal engendré par f_1, \dots, f_k dans $F[u_1, \dots, u_r, X_1, \dots, X_n]$ en respectant un certain ordre monomial sur les monômes en $u_1, \dots, u_r, X_1, \dots, X_n$.

Dans ces deux stratégies on se ramène à calculer un sous-ensemble constructible de \mathcal{P} tel que la spécialisation des paramètres par des valeurs de cet ensemble conduit à une base de Gröbner de l'idéal spécialisé [70, 46, 53, 54, 31, 75]. Notons aussi les bases de Gröbner compréhensive [121, 122] qui partagent l'espace des paramètres en des ensembles constructibles chacun avec une base de Gröbner paramétrique (pas de borne de complexité pour cette construction). D'ailleurs, on peut étudier les conditions sur les paramètres pour que le système n'a pas de solutions, a un nombre fini de solutions, s solutions où s est un entier quelconque, de dimension s ou l'existence de solutions réelles.

2-c- Ensembles caractéristiques et triangulaires :

Pour un système d'équations et d'inéquations polynomiaux paramétrées, les auteurs de [44] décrivent le lieu de consistance \mathcal{U}_1 en le décomposant en un nombre fini d'ensembles constructibles chacun avec un ensemble triangulaire paramétré qui représente les solutions génériques du système. En particulier la dimension du système est constante sur chacun d'eux. D'ailleurs, il n'y a pas une analyse de complexité dans [44].

Des implémentations des méthodes basées sur les ensembles caractéristiques se trouvent dans [120].

3- Solutions réelles :

Des études sur les solutions réelles des systèmes paramétrés se trouvent dans [83, 84, 85] (une étude sur le nombre de solutions réelles d'un système d'égalités et d'inégalités dépendant des paramètres) et dans [41] (une étude des conditions sur les paramètres pour qu'un système paramétrique venant de la chimie admet trois solutions réelles positives). Ainsi dans [124], on trouve un algorithme qui partage \mathcal{P} en des ensembles semi-algébriques chacun avec un nombre constant des racines réelles distinctes et leurs multiplicités pour un polynôme univarié paramétré (pas de borne de complexité pour cet algorithme).

1.3 Nos contributions principales

Nous décomposons cette section en quatre paragraphes. Dans le premier paragraphe, nous précisons le modèle de calcul utilisé dans nos algorithmes.

Dans le deuxième paragraphe, nous décrivons un algorithme de résolution de systèmes algébriques paramétré zéro-dimensionnels qui sera le sujet du chapitre 3. Cet algorithme calcule des U -résultants paramétriques du système paramétré $f_1 = \dots = f_k = 0$ et décrit les solutions du système en utilisant le théorème de l'élément primitif (Shape lemma paramétrique) et l'algorithme de résolution de systèmes algébriques non-paramétrés de [23, 58, 22].

Dans le troisième paragraphe, un algorithme de factorisation absolue de polynômes paramétrés qui formera le contenu du chapitre 4. Cet algorithme utilise une version paramétrisée du lemme de Hensel avec un algorithme d'élimination de quantificateurs dans la théorie des corps algébriquement clos [24] pour réduire le problème de la représentation des facteurs absolument irréductibles à celui de la représentation des solutions d'un certain système polynomial paramétré zéro-dimensionnel.

Le quatrième paragraphe est une illustration du chapitre 5 qui contiendra un algorithme de résolution de systèmes polynomiaux paramétrés de dimensions positives. Cet algorithme est une paramétrisation de l'algorithme de Grigoriev [58] qui décrit toutes les composantes irréductibles d'une variété algébrique par des points génériques *efficaces* et par des systèmes algébriques qui les définissent. Cette paramétrisation n'était pas évidente, il fallait dépasser toutes les difficultés rencontrées pour aboutir à de meilleures bornes sur les degrés des polynômes de la sortie et sur la complexité totale de l'algorithme. Cet algorithme décompose l'espace des paramètres par induction sur la codimension des composantes absolument irréductibles, durant cette induction une intersection d'une certaine variété avec le plan générique conduit à un certain système paramétré zéro-dimensionnel. D'où le besoin d'utiliser les deux algorithmes des chapitres 3 et 4 comme sous-algorithmes de cet algorithme.

1.3.1 Modèle de calcul

Le corps de base F est une extension finie d'une extension purement transcendante de son corps premier H , où $H = \mathbf{Q}$ si $\text{car}(F) = 0$ et $H \supseteq \mathbf{F}_p$ est une extension finie de cardinal assez large si $\text{car}(F) = p > 0$ est un nombre premier, i.e., $F := H(T_1, \dots, T_l)[\eta]$ où T_1, \dots, T_l sont algébriquement indépendants sur H , l'élément η est algébrique, séparable sur le corps $H(T_1, \dots, T_l)$, de polynôme minimal

$$\phi = Z^{\deg(\phi)} + \sum_{0 \leq i < \deg(\phi)} \frac{\phi_i^{(1)}}{\phi^{(2)}} Z^i \in H(T_1, \dots, T_l)[Z]$$

avec $\phi_i^{(1)}, \phi^{(2)} \in H[T_1, \dots, T_l]$ et $\deg(\phi^{(2)})$ est le plus petit possible qu'on peut extraire.

Les polynômes f_1, \dots, f_k de l'entrée de nos algorithmes sont codés en représentation dense, i.e., ils sont donnés par tous leurs coefficients dans le corps H . Chaque f_j , $1 \leq j \leq k$ peut-être représenté d'une manière unique (à un élément près de H^*) sous la forme

$$f_j = \sum_{0 \leq i < \deg_Z(\phi), j_1, \dots, j_r, i_0, \dots, i_n} \frac{a_{i, i_0, \dots, i_n, j_1, \dots, j_r}}{b} \eta^i u_1^{j_1} \dots u_r^{j_r} X_0^{i_0} \dots X_n^{i_n}$$

où $a_{i, i_0, \dots, i_n, j_1, \dots, j_r}, b \in H[T_1, \dots, T_l]$ et $\deg(b)$ est le plus petit possible.

On définit le degré de f_j par rapport aux variables T_1, \dots, T_l par

$$\deg_{T_1, \dots, T_l}(f_j) := \max_{i, i_0, \dots, i_n, j_1, \dots, j_r} \{\deg_{T_1, \dots, T_l}(a_{i, i_0, \dots, i_n, j_1, \dots, j_r}), \deg_{T_1, \dots, T_l}(b)\}$$

De la même façon on définit $\deg_{T_1, \dots, T_l}(\phi)$ le degré de ϕ par rapport à T_1, \dots, T_l .

On désigne par $l(f_j)$ (resp. $l(\phi)$) la longueur de f_j (resp. ϕ), qui est le maximum de longueurs des coefficients (tailles binaires) dans H de monômes en T_1, \dots, T_l des polynômes $a_{i, i_0, \dots, i_n, j_1, \dots, j_r}$ et b (resp. $\phi_i^{(1)}$ et $\phi^{(2)}$) (voir l'appendice pour les propriétés des longueurs).

On suppose qu'on a les bornes suivantes :

$$\deg_{T_1, \dots, T_l, Z}(\phi) \leq d_1, \quad l(\phi) \leq M_1$$

et

$$\deg_{T_1, \dots, T_l}(f_j) \leq d_2, \quad \deg_{X_0, \dots, X_n}(f_j) \leq d, \quad \deg_{u_1, \dots, u_r}(f_j) \leq \delta, \quad l(f_j) \leq M_2.$$

Nous calculons deux sortes des complexités dans nos algorithmes : le nombre d'opérations élémentaires dans le corps H et la complexité binaire totale en considérant les tailles binaires des polynômes intermédiaires des algorithmes. Ces deux complexités sont exprimées en fonction des valeurs suivantes : $k, n, d, r, \delta, l, d_1, d_2, M_1, M_2, p$.

1.3.2 Résolution de systèmes paramétrés zéro-dimensionnels

Nous conservons les mêmes notations de l'introduction et nous introduisons l'ensemble \mathcal{U} des valeurs $a \in \mathcal{P}$ des paramètres tel que le système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est zéro-dimensionnel et n'admet pas de solutions à l'infini, i.e la variété $V^{(a)}$ est un sous-ensemble fini de $P^n(\bar{F})$ avec $V^{(a)} \cap V(X_0) = \emptyset$. Nous résumons cet algorithme de la façon suivante (voir théorème 3.5.3 du chapitre 3) :

1- Algorithme :

On peut produire une décomposition de l'ensemble constructible \mathcal{U} en (au plus)

$$(\delta dd_1)^{O(n^2 r^2)}$$

ensembles constructibles \mathcal{A} deux à deux disjoints qui vérifient :

- 1) Les degrés des équations et des inéquations qui définissent chaque \mathcal{A} par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l ainsi que leurs tailles binaires sont simplement exponentiels en n et r (voir le théorème 3.5.3 du chapitre 3 pour les bornes explicites).
- 2) Le nombre des solutions D est constant sur \mathcal{A} , ce nombre est borné par d^n .
- 3) Le vecteur des multiplicités est constant sur \mathcal{A} et il est calculé par l'algorithme.
- 4) Pour chaque \mathcal{A} , l'algorithme calcule de polynômes $\chi, \psi_1, \dots, \psi_n \in F(u_1, \dots, u_r)[Z]$ de degrés inférieurs ou égale à D . Toute spécialisation des paramètres $a \in \mathcal{A}$ vérifie :
 - Aucun des dénominateurs des coefficients de $\chi, \psi_1, \dots, \psi_n$ ne s'annule en a .
 - Les degrés des coefficients de $\chi, \psi_1, \dots, \psi_n$ par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l ainsi que leurs tailles binaires sont simplement exponentiels en n et r .
 - Une représentation paramétrique des solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est donnée par

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} = \psi_1^{(a)}(\theta) \\ \vdots \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_n}} = \psi_n^{(a)}(\theta) \end{cases}$$

2- Complexité :

Le nombre des opérations élémentaires dans H utilisés dans cet algorithme est borné par

$$(\delta d_2)^{O(r^2(l+1))} (dd_1)^{O(n^2 r^2(l+1))}$$

Sa complexité binaire est

$$(pM_1M_2)^{O(1)} (\delta d_2)^{O(r^2(l+1))} (dd_1)^{O(n^2 r^2(l+1))}.$$

Cette borne de complexité est exponentielle en n et r , analogue à celles obtenues en 2000 par Grigoriev et Vorobjov [60] (par un calcul des bases de Gröbner paramétriques), en 2003 par Schost [109, 110] (opérateur de Newton-Hensel) et en 2004 par Lazard et Rouillier [84] (variétés discriminantes).

Remarque 1.3.1 L'algorithme de [58, 23, 22] (voir aussi le chapitre 2) s'applique sur des systèmes algébriques (non paramétrés) zéro-dimensionnels à coefficients dans le corps $F = H(T_1, \dots, T_l)[\eta]$ défini ci-dessus pour décrire les solutions (en nombre fini) par des représentations univariées polynomiales (RUP). Appliquons directement cet algorithme sur le système paramétré $f_1 = \dots = f_k = 0$ en le considérant à coefficients dans le corps $F' := H(T_1, \dots, T_l, T_{l+1}, \dots, T_{l+r})[\eta]$ où pour tout $1 \leq j \leq r$, $T_{l+j} = u_j$. On obtient une représentation générique de solutions valable seulement pour les valeurs des paramètres qui n'annulent aucun des dénominateurs des expressions qui interviennent dans cette représentation.

1.3.3 Factorisation absolue des polynômes paramétriques

La factorisation absolue des polynômes paramétrés constitue un premier pas vers la résolution des systèmes algébriques paramétrés de dimensions positives (pour le moment considérons le cas $k = 1$, i.e., le système est formé d'une seule équation paramétrée, les composantes absolument irréductibles de l'hypersurface $V(f_1)$ sont définies par les facteurs absolument irréductibles de f_1). Pour $k > 1$, l'utilisation de la factorisation absolue paramétrique dans la résolution du système $f_1 = \dots = f_k = 0$ n'est pas visible pour le moment et sera étudié dans le chapitre 5.

1- Algorithme :

Nous décrivons dans le chapitre 4 un algorithme de factorisation absolue des polynômes paramétrés. Cet algorithme décompose l'espace des paramètres \mathcal{P} en

$$(\delta dd_1)^{O(nr^2d^2)}$$

pièces \mathcal{U} deux à deux disjoints qui sont des ensembles constructibles tel que la factorisation absolue de f_1 est donnée d'une manière uniforme sur chaque pièce. Plus précisément :

1) Chaque \mathcal{U} est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l ainsi que leurs tailles binaires sont simplement exponentiels en n , r et d (voir la section 6 du chapitre 4 pour plus des détails sur les bornes explicites).

2) Pour chaque \mathcal{U} l'algorithme calcule s polynômes $G_1, \dots, G_s \in F(C, u)[X_0, \dots, X_n]$ ($s \leq d$) et un polynôme $\chi \in F(u)[C]$ où C est une nouvelle variable. Pour toute spécialisation des paramètres $a \in \mathcal{U}$, il existe $c \in \overline{F}$, racine de $\chi^{(a)} \in \overline{F}[C]$ (aucun des dénominateurs des coefficients de χ ne s'annule en a) qui vérifie :

- Aucun des dénominateurs des coefficients de G_j ne s'annule en (c, a) .
- Les degrés des coefficients de χ, G_1, \dots, G_s ainsi que leurs tailles binaires sont simplement exponentiels en r et d .

- La factorisation absolue du polynôme $f_1^{(a)} = f_1(a, X_0, \dots, X_n) \in \overline{F}[X_0, \dots, X_n]$ est donnée par :

$$f_1^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c,a)}, \quad G_j^{(c,a)} \text{ est absolument irréductible.}$$

En particulier, le nombre des facteurs absolument irréductibles distincts de $f_1^{(a)}$ est constant sur \mathcal{U} et est égale à s . Par conséquence, si $s = 1$, f_1 est absolument irréductible sur \mathcal{U} .

2- Complexité :

La complexité totale de cet algorithme est

$$(\delta d_2)^{O(r^2 l)} (d d_1)^{O(nr^2 l d^3)}$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(p M_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (d d_1)^{O(nr^2 l d^3)}.$$

Cette borne de complexité est exponentielle en n, r et d .

Exemple 1.3.2 *Considérons le polynôme paramétré suivant :*

$$f = (u^2 + v)x^2 + uxy + vx + uy + v$$

x et y sont deux variables, u et v sont deux paramètres. L'algorithme décompose l'espace des paramètres sous la forme :

$$\mathbb{C}^2 = U_1 \sqcup U_2 \sqcup U_3$$

où $U_1 = \{u^2 + v = 0\}$. Pour tout $(a, b) \in U_1$ on obtient la factorisation absolue :

$$f^{(a,b)} = (x + 1)(ay + b).$$

$U_2 = \{u^2 + v \neq 0, u \neq 0\}$. Pour tout $(a, b) \in U_2$, $f^{(a,b)}$ est absolument irréductible. $U_3 = \{u = 0, v \neq 0\}$. Pour tout $(a, b) \in U_3$, il existe c racine cubique primitive de l'unité (dans ce cas $\chi = C^3 - 1$) qui vérifie

$$f^{(a,b)} = b(x - c)(x - c^2).$$

1.3.4 Résolution de systèmes paramétrés de dimensions positives

On résume dans ce paragraphe le résultat principal du chapitre 5, il s'agit de l'algorithme suivant de résolution de systèmes algébriques paramétrés. Cet algorithme a pour entrée un système paramétré (f_1, \dots, f_k) (avec les notations ci-dessus), codé par une représentation dense et comme sortie une description de toutes les composantes absolument irréductibles des variétés projectives $V^{(a)}$ d'une manière uniforme sur les valeurs a des paramètres (voir théorème 5.2.5 et corollaire 5.7.1 du chapitre 5).

1- Algorithme :

L'algorithme partage l'espace des paramètres \mathcal{P} en (au plus)

$$k(\delta dd_1)^{r^3 d^{O(n^3)}}$$

ensembles constructibles \mathcal{U} deux à deux disjoints vérifiant les propriétés suivantes :

1) Chaque \mathcal{U} est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l ainsi que leurs tailles binaires sont doublement exponentiels en n et simplement exponentiels en r et d (voir théorème 5.2.5 pour les bornes explicites).

2) Pour tout ensemble \mathcal{U} et $a \in \mathcal{U}$, le nombre L des composantes $W_1^{(a)}, \dots, W_L^{(a)}$ absolument irréductibles de la variété projective $V^{(a)} \subset P^n(\overline{F})$ est le même i.e., L est indépendant de a . En plus $L \leq \deg(V^{(a)}) \leq (kd)^{O(n)}$ (inégalité de Bézout [66, 125, 15, 112]).

3) Pour chaque \mathcal{U} , l'algorithme calcule une base Y_0, \dots, Y_n de l'espace des formes linéaires en X_0, \dots, X_n à coefficients dans H . Chaque composante absolument irréductible W parmi W_1, \dots, W_L , de codimension m , est donnée par **un système représentatif paramétrique** et **un point générique efficace paramétrique** au sens suivant :

Système représentatif paramétrique :

Pour chaque \mathcal{U} , l'algorithme calcule des polynômes $\psi_1, \dots, \psi_N \in F(C, u_1, \dots, u_r)[Y_0, \dots, Y_n]$ homogènes en Y_0, \dots, Y_n de degrés $\leq d^{O(m)}$ et un polynôme $\chi \in F(u_1, \dots, u_r)[C]$. Pour tout $a \in \mathcal{U}$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ (les coefficients de χ sont bien définis sur \mathcal{U}) qui vérifient :

- Aucun des dénominateurs des coefficients de ψ_1, \dots, ψ_N ne s'annule en (c, a) .
- $N \leq d^{O(n^2)}$.
- Les polynômes homogènes $\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)} \in \overline{F}[Y_0, \dots, Y_n]$ définissent la variété $W^{(a)}$, i.e.,

$$W^{(a)} = V(\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)}) \subset P^n(\overline{F}).$$

Point générique efficace paramétrique :

- i) La variété $W^{(a)}$ n'est pas contenue dans l'hyperplan $V(Y_0) \subset P^n(\overline{F})$.
- ii) Les fonctions rationnelles $t_1 = \frac{Y_1}{Y_0}, \dots, t_{n-m} = \frac{Y_{n-m}}{Y_0}$ sur $W^{(a)}$ forment une base de transcendance de $\overline{F}(W^{(a)})$ sur \overline{F} .

iii) Pour chaque \mathcal{U} , l'algorithme calcule des polynômes $\phi, B_1, \dots, B_n \in F(C, u_1, \dots, u_r)(t_1, \dots, t_{n-m})[Z]$ et une fonction rationnelle $\theta = \sum_{0 \leq j \leq n} \alpha_j \frac{Y_j}{Y_0}$ avec $0 \leq \alpha_j \leq \deg(W_{v_m}^{(a)}) \leq d^m$. Il calcule aussi une puissance p^ν ($p^\nu = 1$ si $\text{car}(F) = 0$ et $\nu \geq 0$ si $\text{car}(F) = p > 0$). Pour tout $a \in \mathcal{U}$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ vérifiant :

- Aucun des dénominateurs des coefficients de ϕ, B_1, \dots, B_n dans $F(C, u_1, \dots, u_r)$ ne s'annule en (c, a) .

- Un point générique efficace de $W^{(a)}$ (voir [58, 23, 22] et le chapitre 2 pour sa définition) est défini par la représentation univariée polynomiale suivante des éléments de $W^{(a)}$:

$$\phi^{(c,a)}(t_1, \dots, t_{n-m}, \theta) = 0, \begin{cases} \left(\frac{Y_1}{Y_0}\right)^{p^\nu} = B_1^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \\ \vdots \\ \left(\frac{Y_n}{Y_0}\right)^{p^\nu} = B_n^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \end{cases}$$

4) Les degrés des coefficients de ψ_1, \dots, ψ_N et B_1, \dots, B_n ainsi que leurs tailles binaires sont simplement exponentiels en n, r et d tandis que ceux des coefficients de χ et ϕ sont doublement exponentiels en n et simplement exponentiels en r et d (voir théorème 5.2.5 pour les bornes explicites).

Remarque 1.3.3 *On pouvait considérer le système (f_1, \dots, f_k) comme un système à coefficients dans le corps $F' = F(u_1, \dots, u_r)$ de fonctions rationnelles en les paramètres et appliquer ensuite l'algorithme de [58, 23] sur ce système en considérant u_1, \dots, u_r comme de variables algébriquement indépendantes sur H . De cette façon on représente les points génériques efficaces et les équations définissantes de toutes les composantes irréductibles de la variété $V(f_1, \dots, f_k) \subset P^n(\overline{F'})$ par de polynômes à coefficients rationnelles en u_1, \dots, u_r . Alors on peut construire une hypersurface S de l'espace des paramètres sur lequel les dénominateurs de ces coefficients s'annulent identiquement. Pour tout $a \notin S$ on obtient une description de toutes les composantes absolument irréductibles de la variété $V^{(a)}$ (i.e., un point générique efficace avec une famille de polynômes qui définit la composante) par une simple spécialisation des paramètres en a . Par contre pour $a \in S$ l'algorithme ne dit rien sur les composantes absolument irréductibles de $V^{(a)}$. D'où le besoin d'un algorithme qui décrit toutes les composantes absolument irréductibles de toutes les variétés $V^{(a)}$ pour tout $a \in \mathcal{P}$ par des spécialisations simples des paramètres.*

2- Complexité :

La complexité totale de l'algorithme est

$$(\delta d_1 d_2)^{O(r^4(l+1))} d^{r^4(l+1)d^{O(n^3)}}.$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(pM_1M_2)^{O(1)}(\delta d_1d_2)^{O(r^4(l+1))}d^{r^4(l+1)d^{O(n^3)}}.$$

Cette borne de complexité est doublement exponentielle en le nombre n des variables du système paramétré, simplement exponentielle en r et d . Vu qu'une borne inférieure du problème de résolution de systèmes algébriques paramétrés zéro-dimensionnels est doublement exponentielle en n (voir [61] et la section précédente), la borne ci-dessus pour la résolution de systèmes algébriques paramétrés de dimensions positives est donc proche de la borne exacte (i.e., borne inférieure).

Exemple 1.3.4 1) Reprenons l'exemple précédent et considérons l'hypersurface $V = V(f)$ défini par le polynôme

$$f = (u^2 + v)x^2 + uxy + vx + uy + v$$

L'espace des paramètres est décomposé en 3 ensembles constructibles U_1, U_2 et U_3 . Pour tout $(a, b) \in U_1$ l'hypersurface $V^{(a,b)}$ admet deux composantes absolument irréductibles définies par les polynômes $x + 1$ et $ay + b$. Sur U_2 on a une seule composante absolument irréductible car $f^{(a,b)}$ est absolument irréductible. Pour tout $(a, b) \in U_3$ l'hypersurface $V^{(a,b)}$ admet deux composantes absolument irréductibles définies par les polynômes $x - c$ et $x - c^2$ où c est une racine cubique primitive de l'unité.

2) Considérons le système polynomial paramétré suivant apparu dans [13, 121, 44] :

$$\begin{cases} x_4 - u_4 + u_2 = 0 \\ x_4 + x_3 + x_2 + x_1 - u_4 - u_3 - u_1 = 0 \\ x_3x_4 + x_1x_4 + x_2x_3 + x_1x_3 - u_1u_4 - u_1u_3 - u_3u_4 = 0 \\ x_1x_3x_4 - u_1u_3u_4 = 0 \end{cases}$$

où les variables u_1, \dots, u_4 sont les paramètres et les variables x_1, \dots, x_4 sont les inconnus du système.

On peut décomposer l'espace des paramètres \mathbb{C}^4 en 3 ensembles constructibles U_1, U_2 et U_3 qui vérifient :

$$U_1 = \{u_2 - u_4 \neq 0\}, \quad \theta^3 - \alpha\theta^2 + \beta\theta - u_1u_3u_4 = 0, \quad \begin{cases} x_1 = -\frac{1}{u_2 - u_4}\theta^2 + \frac{\alpha}{u_2 - u_4}\theta - \frac{\beta}{u_2 - u_4} \\ x_2 = \frac{1}{u_2 - u_4}\theta^2 - \frac{\alpha}{u_2 - u_4}\theta + \frac{\beta}{u_2 - u_4} \\ x_3 = \theta \\ x_4 = u_4 - u_2 \end{cases}$$

$$U_2 = \{u_2 - u_4 = 0, u_1u_3u_4 \neq 0\}, \quad \text{pas de solutions.}$$

$$U_3 = \{u_2 - u_4 = 0, u_1u_3u_4 = 0\}, \quad \theta^2 - (u_1^2 + u_3^2 + u_4^2 - 2\beta) = 0, \quad \begin{cases} x_1 = -\frac{1}{2}\theta - t + \frac{\alpha}{2} \\ x_2 = t \\ x_3 = \frac{1}{2}\theta + \frac{\alpha}{2} \\ x_4 = 0 \end{cases}$$

où $\alpha = u_1 + u_3 + u_4$, $\beta = u_1u_4 + u_1u_3 + u_3u_4$, $\alpha' = u_1 + u_2 + u_3$ et $\beta' = u_1u_2 + u_1u_3 + u_2u_3 - u_2u_4 + u_2^2$.

Remarquons que pour toute spécialisation (a_1, \dots, a_4) des paramètres dans U_1 , le système associé admet 3 solutions qui correspondent aux 3 racines a_1, a_3 et a_4 de l'équation $\theta^3 - \alpha\theta^2 + \beta\theta - u_1u_3u_4 = 0$. Pour $(a_1, \dots, a_4) \in U_3$ le système associé est de dimension 1.

3- Perturbation :

On peut perturber le système (f_1, \dots, f_k) en introduisant une nouvelle variable ϵ et le nouveau système $(\tilde{f}_1, \dots, \tilde{f}_k)$ défini par :

$$\tilde{f}_i := f_i - \epsilon X_i^d \in F(\epsilon)[u_1, \dots, u_r, X_0, \dots, X_n], \quad 1 \leq i \leq k$$

Ce système forme une intersection complète. Une paramétrisation de l'algorithme de [22] permet de partager l'espace des paramètres en un nombre fini d'ensembles constructibles et de construire toutes ses composantes absolument irréductibles par de systèmes représentatifs paramétriques et par de points génériques efficaces paramétriques. Un passage à la limite $\epsilon \rightarrow 0$ (voir [106]) donne toutes les composantes absolument irréductibles du système d'origine (f_1, \dots, f_k) d'une manière uniforme sur les valeurs des paramètres (i.e., au sens de l'algorithme ci-dessus). La complexité d'une telle construction est plus grande que celle donnée ci-dessus, i.e., cette borne est au moins double-exponentielle en le nombre n des variables.

Chapitre 2

Quelques algorithmes intermédiaires

2.1 Factorisation de polynômes sans paramètres

Considérons un polynôme $f \in F[X_1, \dots, X_n]$ à n variables X_1, \dots, X_n à coefficients dans un corps F . On dit que f est irréductible dans $F[X_1, \dots, X_n]$ (i.e., irréductible sur F) s'il n'existe pas deux polynômes f_1, f_2 non constants dans $F[X_1, \dots, X_n]$ tel que $f = f_1 f_2$. Il est bien connu que f se décompose d'une manière unique (à un facteur près de F^*) en produit d'un nombre fini de polynômes f_1, \dots, f_s , irréductibles sur F . Cette décomposition est appelée la factorisation de f sur F .

Etablir des algorithmes efficaces qui permettent de calculer les facteurs irréductibles d'un certain polynôme f est un problème fondamental en algèbre commutative et en géométrie algébrique (par exemple, une factorisation de f donne les composantes irréductibles $V(f_1), \dots, V(f_s)$ de l'hypersurface $V(f)$ dans l'espace affine F^n).

2.1.1 Factorisation sur le corps des nombres rationnels

Kronecker a factorisé des polynômes univariés à coefficients entiers avec un algorithme de complexité exponentielle en le degré (voir [71, 96]).

En se basant sur l'algorithme de Berlekamp [10, 11] et le lemme de Hensel (voir e.g., [118, 96, 102, 103, 22, 58, 126]), Zassenhaus (voir e.g., [96, 126]) a fait un algorithme de factorisation de polynômes dans $\mathbb{Z}[X]$ mais aussi avec une complexité exponentielle en la taille de l'entrée. Le premier algorithme de factorisation de polynômes univariés sur \mathbb{Q} avec une complexité polynomiale en la taille de l'entrée a été publié en 1982 dans [89] par A.K. Lenstra, H.W. Jr. Lenstra et L. Lovasz (LLL -algorithme). Cette complexité est $d^{12} + d^9 \log^3 l$ où d est le degré du polynôme considéré et l sa taille binaire.

L'utilisation de l'algorithme LLL avec une version multivariée du lemme de Hensel ont conduit en 1982 à un algorithme polynomial de factorisation des polynômes multivariés à coefficients dans \mathbb{Q} par Chistov et Grigoriev [25] (voir aussi [58, 22, 23]).

Quelques mois plus tard en 1982 Kaltofen (voir [74]) a décrit un algorithme déterministe de réduction de la factorisation de polynômes multivariés à celle de polynômes univariés. Cet algorithme a une complexité polynomiale en le degré d et la taille binaire des coefficients du polynôme considéré lorsque le nombre des variables est constant.

2.1.2 Factorisation sur un corps fini

Vers la fin des années 60, Berlekamp [10, 11] a décrit un algorithme probabiliste qui factorise un polynôme univarié à coefficients dans un corps fini à q éléments par des méthodes d'algèbre linéaire avec une complexité polynomiale $O(d^3 \log q)$ où d est le degré de ce polynôme (voir aussi [96]).

Chistov et Grigoriev (voir [25, 58, 22, 23]) ont présenté des algorithmes polynomiaux en la taille de l'entrée pour factoriser des polynômes à n variables à coefficients dans \mathbb{F}_q , i.e., leur complexité est $(d^n \log q)^{O(1)}$. Ces algorithmes sont basés sur le calcul d'un vecteur minimal des réseaux en utilisant l'algorithme LLL de [89].

Von zur Gathen et Kaltofen [119] ont décrit deux algorithmes polynomiaux pour factoriser des polynômes à deux variables à coefficients dans \mathbb{F}_q , le premier algorithme est probabiliste avec une complexité $(d \log q)^{O(1)}$ et le deuxième est déterministe avec une complexité $(dq)^{O(1)}$ où d est le degré du polynôme à factoriser.

La même borne de complexité (i.e., polynomiale) est obtenue en 1983 par Lenstra [90] pour la factorisation des polynômes multivariés à coefficients dans un corps fini.

La complexité de factorisation des polynômes univariés à coefficients dans \mathbb{F}_q est améliorée en 1995 par Kaltofen et Shoup [73] et elle est devenue $O(d^{1.815} \log q)$ par une famille d'algorithmes probabilistes.

Une amélioration sur l'exposant $O(1)$ de ces bornes de complexité est réalisée dans [12] en décrivant un algorithme déterministe avec une complexité $\tilde{O}(d^{\omega+1})$ et un autre algorithme probabiliste avec une complexité $\tilde{O}(d^\omega)$ pour factoriser des polynômes bivariés à coefficients dans \mathbb{F}_q où ω est l'exposant de l'algèbre linéaire [118], i.e., la multiplication de deux matrices carrées d'ordre n se fait en n^ω opérations élémentaires dans le corps de base où $2 < \omega \leq 3$ ($\omega \leq 2.376$ dans [29]).

2.1.3 Factorisation sur une extension algébrique

En 1982, dans leurs travaux sur la décomposition des variétés algébriques en composantes irréductibles, Chistov et Grigoriev (voir [25, 58, 22, 23]) ont décrit un algorithme polynomial de factorisation de polynômes multivariés à coefficients dans un corps qui est une extension finie d'une extension purement transcendante de son corps premier, i.e., le corps $F = H(T_1, \dots, T_l)[\eta]$ introduit au chapitre 1.

Dans le cas où $l = 0$ et F est de caractéristique zéro, i.e., $F = \mathbb{Q}[\eta]$ où η est algébrique sur \mathbb{Q} de polynôme minimal $\phi \in \mathbb{Q}[Z]$. La factorisation d'un polynôme multivarié $f \in \mathbb{Z}[\eta][X_1, \dots, X_n]$, se fait dans un temps polynomial aussi en la taille d'entrée [74, 78, 91], les coefficients des facteurs sont représentés par des polynômes en η de degrés $< \deg(\phi)$. Plus précisément, ce temps est $(h \deg(\phi) d^n)^{O(1)}$ où d est le degré de f en X_1, \dots, X_n et h est la taille binaire maximale des coefficients de f dans \mathbb{Z} .

2.1.4 Factorisation absolue

Un polynôme $f \in F[X_1, \dots, X_n]$ est dit absolument irréductible s'il est irréductible sur la clôture algébrique \bar{F} de F , ceci est équivalent à ce que f est irréductible sur toute

extension algébrique de F . La factorisation absolue de f est sa décomposition en produit de facteurs absolument irréductibles.

Deux stratégies sont adoptées pour factoriser absolument un certain polynôme f :

1- Un calcul symbolique :

Il s'agit de trouver une extension primitive $F[\alpha]$ de F représentée par le polynôme minimal de α sur F , qui contient les coefficients de tous les facteurs absolument irréductibles de f .

En 1983, Chistov et Grigoriev [23] (voir aussi [22]) ont proposé un algorithme avec une complexité polynomiale de réduction de la factorisation absolue à la factorisation sur le corps de base. Cet algorithme est combiné avec un autre algorithme polynomial de factorisation sur le corps de base pour produire un algorithme polynomial de factorisation absolue.

En 2003 Gao [42] propose un algorithme probabiliste de factorisation absolue de polynômes bivariés à coefficients dans un corps de caractéristique zéro ou de caractéristique $p > d(d-1)$ où d est le degré des polynômes à factoriser. Cet algorithme est basé sur la résolution de systèmes linéaires larges et sur la factorisation de polynômes univariés sur le corps de base, il se fait avec $\tilde{O}(d^5)$ opérations élémentaires. Cette borne de complexité était améliorée par Chèze et Lecerf [20, 19] et elle est devenue $\tilde{O}(d^4)$ par un algorithme déterministe et une complexité sous-quadratique $\tilde{O}(d^{(\omega+3)/2})$ en la taille d^2 du polynôme d'entrée par un algorithme probabiliste. Ces algorithmes sont implantés et ils sont efficaces en pratique [19].

2- Un calcul numérique :

Il s'agit de calculer une approximation des coefficients des facteurs absolument irréductibles de f lorsque $F = \mathbb{Q}$. Soit f_1, \dots, f_s les facteurs absolument irréductibles de $f \in \mathbb{Q}[X, Y]$ et $\tilde{f}_1 \cdots \tilde{f}_s \in \mathbb{C}[X, Y]$. On dit que $f \approx \tilde{f}_1 \cdots \tilde{f}_s$ est une factorisation absolue approximative de f avec une précision ϵ si pour tout $1 \leq i \leq s$ les coefficients de \tilde{f}_i sont des approximations numériques de ceux de f_i avec une précision ϵ , i.e., pour tout $1 \leq i \leq s$, $\|f_i - \tilde{f}_i\|_\infty < \epsilon$ où $\|g\|_\infty$ est le maximum des valeurs absolues des coefficients de g .

Chèze et Galligo [21, 19] ont établi un algorithme qui reconstruit les facteurs exactes à partir des facteurs approximatifs, i.e., les facteurs f_1, \dots, f_s à partir des facteurs $\tilde{f}_1 \cdots \tilde{f}_s$.

Plusieurs algorithmes géométriques effectuent une approximation numérique des coefficients des facteurs des polynômes bivariés à coefficients rationnels [19, 21, 30, 43, 116].

2.2 Résolution de systèmes algébriques sans paramètres

2.2.1 Historique

Supposons qu'on a une famille de polynômes $f_1, \dots, f_k \in F[X_1, \dots, X_n]$, de degré borné par d chacun et on cherche à trouver les zéros communs de ces polynômes dans une clôture algébrique \overline{F} de F . Nous verrons comment représenter ces zéros dans les exemples suivants :

Exemple 2.2.1 *Soit le système linéaire suivant*

$$\begin{cases} X + 2Y - Z - 3 &= 0 \\ X - Y - 4Z + 9 &= 0 \\ Y + Z - 4 &= 0 \end{cases}$$

Ce système admet une infinité de solutions représentées par la paramétrisation suivante :

$$\begin{cases} X &= 3t - 5 \\ Y &= -t + 4 \\ Z &= t \end{cases}$$

où t est un paramètre. Cela veut dire que Z joue le rôle d'un paramètre, les autres variables X et Y sont exprimées en fonction de Z .

Peut-on généraliser cette représentation pour un système non-linéaire ?

Exemple 2.2.2 *Soit le système non-linéaire suivant*

$$\begin{cases} XYZ^2 - XY + 1 &= 0 \\ -X^2Y + X - 1 &= 0 \\ X^2 + Z + 1 &= 0 \end{cases}$$

Ce système est équivalent au système suivant (par un calcul d'une base de Gröbner en respectant l'ordre lexicographique) :

$$\begin{cases} Z^4 + Z^3 - Z^2 - Z + 1 &= 0 \\ Y + Z^3 + Z^2 - 1 &= 0 \\ X - Z^3 - 2Z^2 + 1 &= 0 \end{cases}$$

Ce dernier système est zéro-dimensionnel et ses solutions sont données par la représentation suivante :

$$\theta^4 + \theta^3 - \theta^2 - \theta + 1 = 0, \quad \begin{cases} X &= \theta^3 + 2\theta^2 - 1 \\ Y &= -\theta^3 - \theta^2 + 1 \\ Z &= \theta \end{cases}$$

Exemple 2.2.3 Soit le système

$$\begin{cases} X^2 + XY + Y - 1 & = 0 \\ -X^2 + Y^2 + 2X - 1 & = 0 \\ -3X + Y + 4Z + 3 & = 0 \end{cases}$$

La variété définie par ce système se décompose en deux composantes irréductibles V_1 (de dimension 0) et V_2 (de dimension 1) qui sont définies par :

$$V_1 : \begin{cases} X + 1 & = 0 \\ -X + Z & = 0 \\ -X + Y + 1 & = 0 \end{cases}$$

$$V_2 : \begin{cases} X + Y - 1 & = 0 \\ Y + Z & = 0 \end{cases}$$

Les polynômes f_1, \dots, f_k définissent une variété algébrique $V = V(f_1, \dots, f_k) \subset \overline{F}^n$. Les variétés algébriques sont des objets fondamentaux en géométrie algébrique, leur décomposition en des objets géométriques plus simples (i.e, leurs éléments dans le cas zéro-dimensionnel et les composantes irréductibles dans le cas de dimension positive) est un problème naturel et intéressant qui rend leur manipulation plus facile pour faire de calculs géométriques.

La théorie d'élimination permet de résoudre de systèmes polynomiaux en éliminant les variables (l'une après l'autre [117] ou toutes à la fois [24]) et en réduisant ces systèmes à d'autres systèmes équivalents et plus faciles à résoudre par une méthode qui calcule les racines de polynômes univariés. Cette théorie a été étudiée par Macaulay [93] dans le cas projectif et $k = n$, i.e., f_1, \dots, f_n sont de polynômes homogènes en X_1, \dots, X_n (voir chapitre 3). Macaulay a calculé un polynôme en les coefficients du système étudié, appelé le résultant du système tel que son annulation est équivalent au fait que le système admet une solution dans l'espace projectif $(n - 1)$ -dimensionnel $P^{n-1}(\overline{F})$.

1- Résolution de systèmes algébriques zéro-dimensionnels :

Pour tout $1 \leq i \leq k$, considérons \tilde{f}_i l'homogénéisation de f_i par l'introduction d'une nouvelle variable X_0 . Dans le cas où le système $\tilde{f}_1 = \dots = \tilde{f}_k = 0$ admet un nombre fini de solutions dans $P^n(\overline{F})$, la théorie d'élimination calcule un autre polynôme, appelé le u -résultant du système, noté R , à coefficients dans F , homogène en des nouvelles variables U_0, \dots, U_n tel qu'il existe une correspondance bijective entre les solutions du système dans $P^n(\overline{F})$ (comptées avec leurs multiplicités) d'une part et les facteurs linéaires de R à coefficients dans \overline{F} d'autre part, i.e., pour tout facteur linéaire $L = \xi_0 U_0 + \dots + \xi_n U_n$ de R dans $\overline{F}[U_0, \dots, U_n]$, le point $(\xi_0 : \dots : \xi_n) \in P^n(\overline{F})$ est une solution du système $\tilde{f}_1 = \dots = \tilde{f}_k = 0$, sa multiplicité est égale à celle de L en tant que facteur de R (voir [93, 117, 81, 58, 17] et le chapitre 3 pour des algorithmes qui calculent le u -résultant).

Une borne de complexité double-exponentielle d^{2^n} est connue dans les travaux de Kronecker (voir e.g., Collins [28] et Heintz [66]) pour la résolution de systèmes zéro-dimensionnels. Lazard [81] a calculé le u-résultant des systèmes zéro-dimensionnels d'équations homogènes par une méthode basée sur la réduction des matrices en exécutant $d^{O(n)}$ opérations élémentaires, polynomial en le nombre de solutions.

Dans le cas où F est une extension finie d'une extension purement transcendante de son corps premier H (i.e., le corps introduit au chapitre 1), Grigoriev [58] (voir aussi [22, 23]) a décrit un algorithme qui combine le u -résultant du système $\tilde{f}_1 = \dots = \tilde{f}_k = 0$ avec le lemme de l'élément primitif (Shape lemma) [50, 76, 2] pour décomposer l'ensemble fini de solutions du système en de classes de conjugaison C_1, \dots, C_s sur F tels que pour chaque classe C l'algorithme calcule des polynômes $\phi, B_0, \dots, B_n \in F[Z]$, un indice j_0 , $0 \leq j_0 \leq n$ et une puissance p^ν de la caractéristique p de F qui vérifient :

- ϕ est séparable et irréductible sur F .
- Une représentation univariée polynomiale de solutions du système dans C est donnée par :

$$\phi(\theta) = 0, \quad \left\{ \begin{array}{l} \left(\frac{X_0}{X_{j_0}} \right)^{p^\nu} = B_0(\theta) \\ \vdots \\ \left(\frac{X_n}{X_{j_0}} \right)^{p^\nu} = B_n(\theta) \end{array} \right.$$

i.e., toute solution $(\xi_0 : \dots : \xi_n) \in P^n(\overline{F})$ du système dans C vérifie $\xi_{j_0} \neq 0$ et les fractions $\left(\frac{\xi_j}{\xi_{j_0}} \right)$ sont obtenues par un calcul des racines du polynôme univarié ϕ dans \overline{F} et par extraction des racines p^ν -ème d'éléments de \overline{F} . En particulier, le cardinal de C est égal au degré de ϕ en Z . La complexité de cet algorithme est $pd^{O(n)}$ polynomiale en la taille de la sortie.

Cette manière de représenter les solutions des systèmes algébriques zéro-dimensionnels est devenue célèbre par Fabrice Rouillier [108] (voir aussi [2, 8]) sous le nom de RUR (Représentation Univariée Rationnelle). Cette représentation exprime les solutions du système $f_1 = \dots = f_k = 0$ comme des fonctions rationnelles des racines d'un polynôme univarié tout en conservant les multiplicités et les racines réelles, i.e.,

$$\phi(\theta) = 0, \quad \left\{ \begin{array}{l} X_1 = \frac{B_1(\theta)}{\phi'(\theta)} \\ \vdots \\ X_n = \frac{B_n(\theta)}{\phi'(\theta)} \end{array} \right.$$

où $\phi, B_1, \dots, B_n \in F[Z]$, ϕ est séparable dans $F[Z]$. La complexité de la construction d'une telle représentation est $d^{O(n)}$ polynomiale en le nombre des solutions du système.

En 1965, Bruno Buchberger (voir e.g. [13]) a inventé les bases de Gröbner qui permettent de transformer le système étudié à un système triangulaire qui peut-être résolu par la recherche des racines des polynômes univariés. Cette méthode est une généralisation de l'algorithme d'élimination de Gauss à des systèmes non-linéaires et de l'algorithme d'Euclide à des polynômes multivariés [27, 82]. Pour une bonne exposition des bases de Gröbner et leurs applications voir les livres de Cox et. al. [31, 32]. La complexité du calcul d'une base de Gröbner d'un idéal zéro-dimensionnel est $d^{O(n)}$, polynomiale en la taille de l'entrée du système définissant l'idéal [82, 77, 39]. Cette borne de complexité est améliorée dans [64] et elle est devenue polynomiale en $\max\{S, D^n\}$ où S est la taille de l'entrée pour la représentation dense et D est la moyenne arithmétique des degrés des polynômes d'entrée.

Si les polynômes de l'entrée sont représentés par un programme d'évaluation (Straight-line program [76]), des algorithmes probabilistes existent dans [51, 49, 67] avec des complexités polynomiales qui calculent une résolution géométrique du système.

La théorie des ensembles triangulaires [86, 4, 5] et les ensembles caractéristiques [120] permettent de décomposer l'ensemble de solutions du système étudié en un nombre fini d'ensembles de zéros d'ensembles triangulaires.

Si le système $f_1 = \dots = f_k = 0$ admet un nombre fini de solutions dans \overline{F}^n alors l'algèbre $A = F[X_1, \dots, X_n]/(f_1, \dots, f_k)$ est de dimension finie sur F et donc on peut manipuler des méthodes d'algèbre linéaire pour calculer les solutions du système.

Une méthode simple de résolution des systèmes zéro-dimensionnels consiste à calculer les valeurs propres des endomorphismes Φ_{X_i} de l'algèbre A , pour tout $1 \leq i \leq n$, où Φ_{X_i} est la multiplication par X_i dans A . Il suffit d'évaluer les polynômes f_1, \dots, f_k en $(\lambda_1, \dots, \lambda_n)$ où λ_i est une valeur propre de Φ_{X_i} , en tenant compte que pour tout $f \in F[X_1, \dots, X_n]$, les valeurs propres de Φ_f sont les $f(x)$ où x est une solution du système $f_1 = \dots = f_k = 0$. La complexité de cette méthode est parfaitement large.

D'autres méthodes consistent à calculer les espaces propres des endomorphismes de multiplication de A [6, 99, 32, 35].

2- Résolution de systèmes algébriques de dimensions positives :

Dans le cas où le système $f_1 = \dots = f_k = 0$ est de dimension positive, sa résolution revient à calculer les composantes irréductibles de la variété algébrique $V = V(f_1, \dots, f_k)$.

En 1983, Chistov et Grigoriev [23, 22, 58] ont décrit un algorithme qui décompose une variété projective arbitraire à ses composantes irréductibles. Chaque composante est donnée par les deux voies suivantes :

i) Un point générique (voir [125, 101, 79, 23, 22, 58] et le paragraphe suivant).

ii) Une famille finie de polynômes homogènes qui définit cette composante.

Dans le paragraphe suivant, nous détaillons les grandes lignes de leur algorithme géométrique effectif qui sera paramétrisé dans le chapitre 5 pour résoudre des systèmes algébriques paramétrés. Notons que sa complexité est polynomiale en d^{n^2} .

En 1988, Gianni et. al. [45] utilisent les bases de Gröbner et les idéaux quotients dans l'anneau polynomial $F[X_1, \dots, X_n]$ pour calculer une décomposition primitive de l'idéal $I = \langle f_1, \dots, f_k \rangle$ (voir aussi [31, 35]). La factorisation des polynômes f_1, \dots, f_k , combinée avec l'algorithme de Buchberger permet aussi de décomposer la variété V [56, 57].

Giusti et Heintz [48] ont établi en 1990 un algorithme bien parallélisable qui décompose la variété V en composantes équidimensionnelles et en composantes irréductibles avec une complexité séquentielle d'ordre $k^5 d^{O(n^2)}$ et en 1993 [50] un algorithme bien parallélisable aussi qui calcule la dimension, le degré géométrique et les points isolés de la variété V dans un temps séquentiel polynomial en la taille de la sortie. Elkadi et Mourrain [36] proposent aussi un algorithme probabiliste basé sur les matrices Bézoutiennes avec la même borne de complexité.

Giusti et. al. [49, 52] ont calculé une résolution géométrique qui donne une représentation paramétrique de solutions qui est une généralisation du lemme de l'élément primitif et de la représentation univarié rationnelle au cas dimension positive. Notons qu'une représentation des composantes irréductibles par des points génériques [23, 22, 58] donne aussi une telle représentation (voir le paragraphe suivant).

Récemment Lecerf [87, 88] décrit un algorithme qui calcule une résolution géométrique de chaque composante équidimensionnelle de la variété V avec une complexité polynomiale en kd^n .

En 2002, Jeronimo et Sabia [69] proposent un algorithme probabiliste qui représente chaque composante équidimensionnelle de V par une famille de $n + 1$ polynômes de degrés $\leq d^n$. Ces polynômes sont codés par un programme d'évaluation de longueur polynomial en kd^n .

Sommese et. al. [115] proposent un algorithme numérique pour la décomposition de la variété V en composantes irréductibles. Chaque composante W est donnée par les deux voies suivantes :

- Un sous-ensemble fini des points de W de cardinal égale au degré de W qui est calculé par l'algorithme.

- Une famille de polynômes qui la définit comme dans ii) ci-dessus.

En particulier, l'algorithme calcule l'ensemble des points isolés de V .

2.2.2 Algorithme de Chistov-Grigoriev

Nous montrons dans ce paragraphe les entrées et les sorties de l'algorithme de Chistov-Grigoriev [23, 22, 58] avec sa borne de complexité. Le corps de base de cet algorithme (i.e., le corps des coefficients des polynômes du système d'entrée f_1, \dots, f_k) est le corps $F = H(T_1, \dots, T_l)[\eta]$ introduit au chapitre 1. On suppose que $f_1, \dots, f_k \in F[X_0, \dots, X_n]$ sont homogènes en X_0, \dots, X_n et qu'ils sont codés en représentation dense par leurs vecteurs des coefficients dans le corps H . On suppose aussi qu'on a les mêmes bornes sur les degrés et les tailles binaires de polynômes f_1, \dots, f_k qu'au chapitre 1, i.e., pour tout $1 \leq j \leq k$

$$\deg_{T_1, \dots, T_l}(f_j) \leq d_2, \quad \deg_{X_0, \dots, X_n}(f_j) \leq d, \quad l(f_j) \leq M_2.$$

et

$$\deg_{T_1, \dots, T_l, Z}(\phi) \leq d_1, \quad l(\phi) \leq M_1$$

où ϕ est le polynôme minimal de η sur le corps $H(T_1, \dots, T_l)$. La taille binaire de f_j (resp. ϕ), notée $l(f_j)$ (resp. $l(\phi)$), est le maximum de longueurs binaires des coefficients dans H de monômes en T_1, \dots, T_l dans f_j (resp. ϕ).

Notons par $F^{p^{-\infty}}$ l'extension purement inséparable maximale de F , i.e.,

$$F^{p^{-\infty}} = \bigcup_{\nu \in \mathbf{N}} F^{p^{-\nu}}$$

où

$$F^{p^{-\nu}} := \{\alpha \in \overline{F}, \quad \alpha^{p^\nu} \in F\}$$

où $p = \text{car}(F)$. Si $\text{car}(F) = 0$ alors $F^{p^{-\infty}} := \overline{F}$ (voir [79]).

Toutes les bornes sur les degrés des polynômes intermédiaires et sur la complexité binaire totale de cet algorithme sont mesurées en fonction des valeurs suivantes : $k, d, n, l, d_1, d_2, M_1, M_2, p$.

Dans la suite nous rappelons la notion des points génériques [125, 101, 79, 23, 22, 58] dans les deux cas affine et projective afin que nous décrivions le résultat fondamental de l'algorithme qui consiste à la description de toutes les composantes irréductibles de la variété projective $V = V(f_1, \dots, f_k) \subset P^n(\overline{F})$.

1- Points génériques :

1-a- Cas d'une variété affine :

Nous distinguons deux types des points génériques, les F -points génériques [101] et les points génériques *efficaces* [23, 22, 58] et nous verrons que le deuxième conduit au premier (théorème 2.2.7).

Soit $V \subset \overline{F}^n$ une variété affine définie et irréductible sur F , l'anneau $F[V]$ des fonctions polynomiales sur V est isomorphe à l'anneau quotient $F[X_1, \dots, X_n]/I(V) = F[x_1, \dots, x_n]$ où $I(V) \subset F[X_1, \dots, X_n]$ est l'idéal premier de $F[X_1, \dots, X_n]$ formé par les polynômes qui s'annulent identiquement sur V et pour tout $1 \leq i \leq n$, x_i est la classe de X_i modulo $I(V)$, le point $x = (x_1, \dots, x_n)$ est appelé le F -point générique canonique de V .

D'une manière générale, un F -point générique de V est défini par :

Définition 2.2.4 *Un point $x \in V$ est dit un F -point générique de V si tout polynôme $f \in F[X_1, \dots, X_n]$ qui s'annule en x , il s'annule en tout point de V (i.e., f s'annule identiquement sur V).*

Exemple 2.2.5 *Soit $g_2, \dots, g_n \in \mathbf{Q}[X_1]$ et $V \subset \mathbf{C}^n$ la variété affine définie sur \mathbf{Q} par :*

$$V = V(X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$$

L'idéal $(X_2 - g_2(X_1), \dots, X_n - g_n(X_1)) \subset \mathbf{Q}[X_1, \dots, X_n]$ est un idéal premier car il est le noyau de l'homomorphisme suivant :

$$\begin{aligned} \mathbf{Q}[X_1, \dots, X_n] &\longrightarrow \mathbf{Q}[X_1] \\ X_1 &\longrightarrow X_1 \\ X_i &\longrightarrow g_i(X_1), \quad 2 \leq i \leq n. \end{aligned}$$

Donc V est définie et irréductible sur \mathbf{Q} . Le point $(\pi, g_2(\pi), \dots, g_n(\pi)) \in V$ est un \mathbf{Q} -point générique de V . En général, pour tout $\alpha \in \mathbf{C}$ transcendant sur \mathbf{Q} , le point $(\alpha, g_2(\alpha), \dots, g_n(\alpha)) \in V$ est un \mathbf{Q} -point générique de V .

Le corps $F(V)$ des fonctions rationnelles sur V est le corps de fraction de l'anneau intègre $F[V]$, alors $F(V) = F(x_1, \dots, x_n)$.

Notons que si $m = \text{codim}(V)$ alors le degré de transcendance de $F(V)$ sur F est $\text{degtr}_F F(V) = \dim(V) = n - m$, soit t_1, \dots, t_{n-m} une base de transcendance de $F(V)$ sur F alors $F(V)$ est une extension finie de $F(t_1, \dots, t_{n-m})$. Soit p^ν une puissance maximale ($\nu \geq 0$), $x_i^{p^\nu}$ est séparable sur $F(t_1, \dots, t_{n-m})$ pour tout $1 \leq i \leq n$ ($p^\nu = 1$ si $\text{car}(F) = 0$) alors $F(x_1^{p^\nu}, \dots, x_n^{p^\nu})$ est une extension finie et séparable de $F(t_1, \dots, t_{n-m})$.

Définition 2.2.6 *Un point générique efficace de V est défini par l'existence de l'isomorphisme de corps suivant*

$$\tau : F(t_1, \dots, t_{n-m})[\theta] \longrightarrow F(x_1^{p^\nu}, \dots, x_n^{p^\nu}) \subset F(V)$$

où θ est un élément primitif de l'extension $F(x_1^{p^\nu}, \dots, x_n^{p^\nu})$ sur $F(t_1, \dots, t_{n-m})$, θ est algébrique séparable sur $F(t_1, \dots, t_{n-m})$ de polynôme minimal $\Phi(Z)$.

L'existence d'un point générique efficace de V (i.e., d'un tel isomorphisme de corps) donne une représentation paramétrique rationnelle des éléments de V (analogue à celle obtenue par une résolution géométrique [52, 47, 87, 88]) de la façon suivante :

$$\Phi(t_1, \dots, t_{n-m}, \theta) = 0, \quad \begin{cases} X_1^{p^\nu} = \frac{\phi_1(t_1, \dots, t_{n-m}, \theta)}{\psi(t_1, \dots, t_{n-m})} \\ \vdots \\ X_n^{p^\nu} = \frac{\phi_n(t_1, \dots, t_{n-m}, \theta)}{\psi(t_1, \dots, t_{n-m})} \end{cases}$$

où $\phi_i \in F[t_1, \dots, t_{n-m}, Z]$, $0 \neq \psi \in F[t_1, \dots, t_{n-m}]$ et $\deg_Z \phi_i < \deg_Z \Phi$ pour tout $1 \leq i \leq n$.

Dans le cas où V est fini ($\dim(V) = 0$ et $m = n$), on obtient une représentation paramétrique polynomiale des éléments de V :

$$\Phi(\theta) = 0, \quad \begin{cases} X_1^{p^\nu} = \phi_1(\theta) \\ \vdots \\ X_n^{p^\nu} = \phi_n(\theta) \end{cases}$$

où $\phi_i \in F[Z]$ et $\deg_Z \phi_i < \deg_Z \Phi$ pour tout $1 \leq i \leq n$.

Le théorème suivant montre qu'un point générique efficace est un F -point générique.

Théorème 2.2.7 *Si \overline{F} a un degré de transcendance infini sur F , alors tout point générique efficace de V est un F -point générique de V .*

Preuve. Il existe un isomorphisme σ de $F(x_1^{p^\nu}, \dots, x_n^{p^\nu})$ sur un sous-corps de \overline{F} . Le point $a = (a_1, \dots, a_n)$ où $a_i = \sigma(x_i^{p^\nu}) \in \overline{F}$ est un F -point générique de V . En effet, pour tout polynôme $f \in I(V)$ on a

$$f(a_1, \dots, a_n) = \sigma\left(f(x_1^{p^\nu}, \dots, x_n^{p^\nu})\right) = \sigma\left(f^{p^\nu}(x_1, \dots, x_n)\right) = 0 \text{ dans } \overline{F}$$

car $f(x_1, \dots, x_n) = 0$ dans $F(V)$, ce qui montre que $a \in V$. D'autre part, soit $f \in F[X_1, \dots, X_n]$, supposons que f ne s'annule pas identiquement sur V alors $f \notin I(V)$, ce qui implique que $f(x_1, \dots, x_n) \neq 0$ dans $F(V)$. Donc

$$f(a_1, \dots, a_n) = \sigma\left(f^{p^\nu}(x_1, \dots, x_n)\right) \neq 0 \text{ dans } \overline{F}$$

car σ est injectif. D'où a est un F -point générique de V .

1-b- Cas d'une variété projective :

Soit $W \subset P^n(\overline{F})$ une variété projective non vide définie et irréductible sur F , $F[W] \cong F[X_0, X_1, \dots, X_n]/I(W) = F[x_0, x_1, \dots, x_n]$ où $I(W)$ est l'idéal homogène premier de $F[X_0, X_1, \dots, X_n]$ formé par les polynômes qui s'annulent identiquement sur W et pour tout $0 \leq i \leq n$, $x_i \equiv X_i \pmod{I(W)}$, le point $x = (x_0, x_1, \dots, x_n)$ est appelé le F -point générique canonique de W , ce point est non nul car W est non vide.

De la même manière qu'au cas affine, on peut aussi définir un F -point générique de W comme étant un point de W tel que tout polynôme homogène de $F[X_0, X_1, \dots, X_n]$ qui s'annule en ce point, il s'annule identiquement sur W .

Le corps $F(W)$ des fonctions rationnelles sur W est le sous-corps du corps de fraction de l'anneau intègre $F[W]$ formé par les quotients $\frac{g}{h}$ où g, h sont des polynômes homogènes dans $F[X_0, X_1, \dots, X_n]$ de même degré et $h \notin I(W)$, alors

$$F(W) = F\left(\frac{x_i}{x_j}, 0 \leq i, j \leq n\right) = F\left(\frac{x_0}{x_s}, \dots, \frac{x_n}{x_s}\right) \text{ où } x_s \neq 0 \ (X_s \notin I(W))$$

Considérons $m = \text{codim}(W)$, soit t_1, \dots, t_{n-m} une base de transcendance de $F(W)$ sur F . Un point générique *efficace* de la variété W est défini par l'isomorphisme de corps suivant :

$$\tau : F(t_1, \dots, t_{n-m})[\theta] \longrightarrow F\left(\frac{X_{j_1}}{X_s}, \dots, \frac{X_{j_{n-m}}}{X_s}, \left(\frac{X_0}{X_s}\right)^{p^\nu}, \dots, \left(\frac{X_n}{X_s}\right)^{p^\nu}\right) \subseteq F(W) \quad (2.1)$$

où $0 \leq s \leq n$ est choisi de telle manière que la variété W n'est pas contenue dans l'hyperplan défini par l'équation $X_s = 0$, θ est algébrique séparable sur le corps $F(t_1, \dots, t_{n-m})$, de polynôme minimal $\Phi(Z) \in F(t_1, \dots, t_{n-m})[Z]$, $lc_Z(\Phi) = 1$. En plus $\theta = \sum_j \alpha_j \frac{X_j}{X_s}$ où $\alpha_j \in \mathbb{Z}$ et $0 \leq \alpha_j \leq \deg(W)$, les éléments $\frac{X_j}{X_s}$ sont des fonctions rationnelles sur W , $p^\nu = 1$ si $\text{car}(F) = 0$ et $\nu \geq 0$ si $\text{car}(F) = p > 0$.

Cet isomorphisme donne une représentation paramétrique rationnelle des éléments de V sous la forme :

$$\Phi(t_1, \dots, t_{n-m}, \theta) = 0, \quad \begin{cases} \left(\frac{X_0}{X_s}\right)^{p^\nu} = \frac{\phi_0(t_1, \dots, t_{n-m}, \theta)}{\psi(t_1, \dots, t_{n-m})} \\ \vdots \\ \left(\frac{X_n}{X_s}\right)^{p^\nu} = \frac{\phi_n(t_1, \dots, t_{n-m}, \theta)}{\psi(t_1, \dots, t_{n-m})} \end{cases}$$

où $\phi_j \in F[t_1, \dots, t_{n-m}, Z]$, $0 \neq \psi \in F[t_1, \dots, t_{n-m}]$ et $\deg_Z \phi_j < \deg_Z \Phi$ pour tout $0 \leq j \leq n$.

A chaque choix de $\tau_1, \dots, \tau_{n-m}$ dans \overline{F} qui n'annulent pas ni ψ , ni les dénominateurs des coefficients du polynôme univarié $\Phi(Z) \in F(t_1, \dots, t_{n-m})[Z]$, θ_0 racine de

$\Phi^{(\tau_1, \dots, \tau_{n-m})}(Z) \in \overline{F}[Z]$ dans \overline{F} , on obtient un point de W par extraction des racines p^ν -ème d'éléments de \overline{F} .

On peut démontrer un résultat analogue au théorème 2.2.7 qui caractérise l'idéal $I(W) \subset F[X_0, \dots, X_n]$ et qui est donné par le lemme 2.7 de [58] :

Lemme 2.2.8 *Soit $\psi \in F[X_0, \dots, X_n]$ un polynôme homogène, ψ s'annule identiquement sur W (i.e., $\psi \in I(W)$) si et seulement si $\psi^{p^\nu} \left(\frac{X_0}{X_s}, \frac{X_1}{X_s}, \dots, \frac{X_n}{X_s} \right) = 0$ dans le corps $F(t_1, \dots, t_{n-m})[\theta]$ en utilisant l'isomorphisme (2.1).*

Preuve. On a $\psi^{p^\nu} \left(\frac{X_0}{X_s}, \frac{X_1}{X_s}, \dots, \frac{X_n}{X_s} \right) = \psi \left(\left(\frac{X_0}{X_s} \right)^{p^\nu}, \left(\frac{X_1}{X_s} \right)^{p^\nu}, \dots, \left(\frac{X_n}{X_s} \right)^{p^\nu} \right) = P(t_1, \dots, t_{n-m}, \theta)$ pour un certain $P \in F(t_1, \dots, t_{n-m})[\theta]$ en utilisant l'isomorphisme (2.1). Alors $\psi \in I(W)$ si et seulement si $0 = \psi \left(\frac{X_0}{X_s}, \frac{X_1}{X_s}, \dots, \frac{X_n}{X_s} \right) \in F(W)$ et ceci est équivalent au fait que $P(t_1, \dots, t_{n-m}, \theta) = 0$.

Pour vérifier si une variété $W \subset P^n(\overline{F})$ définie et irréductible sur F , donnée par un point générique *efficace*, est incluse dans une composante de la variété $V = V(f_1, \dots, f_k)$, on utilise la procédure suivante :

Test : Pour une valeur de i allant de 1 à k , on calcule $f_i^{p^\nu} \left(\frac{X_0}{X_s}, \dots, \frac{X_n}{X_s} \right) \in F(t_1, \dots, t_{n-m})[\theta]$ par l'isomorphisme (2.1). Si pour un certain i cette valeur n'est pas nulle alors W n'est pas contenue dans une composante de V et si on obtient des zéros pour tout $1 \leq i \leq k$ alors W est incluse dans une composante de V .

2- Algorithme :

L'algorithme décompose la variété projective $V(f_1, \dots, f_k) \subset P^n(\overline{F})$ en ses composantes irréductibles W qui sont définies et irréductibles sur le corps $F^{p^{-\infty}}$. Chaque W de codimension m est représentée par les deux voies suivantes :

i) L'algorithme calcule un point générique *efficace* de W , i.e., il produit une base de transcendance t_1, \dots, t_{n-m} de $F(W)$ sur F , un élément algébrique θ séparable sur le corps $F(t_1, \dots, t_{n-m})$ avec son polynôme minimal $\Phi(Z) \in F(t_1, \dots, t_{n-m})[Z]$ et les expressions de fonctions rationnelles $\left(\frac{X_j}{X_s} \right)^{p^\nu}$, $0 \leq j \leq n$ par l'isomorphisme τ ci-dessus avec les bornes suivantes :

$$- p^\nu \leq d^{2m}, \deg_Z(\Phi) \leq \deg(W) \leq d^m.$$

$$- \deg_{T_1, \dots, T_l, t_1, \dots, t_{n-m}}(\Phi), \deg_{T_1, \dots, T_l, t_1, \dots, t_{n-m}}(\phi_j), \deg_{T_1, \dots, T_l, t_1, \dots, t_{n-m}}(\psi) \leq d_2(d^m d_1)^{O(1)}.$$

- Les tailles binaires de coefficients de Φ, ϕ_j, ψ sont données par

$$l(\Phi), l(\phi_j), l(\psi) \leq \left(M_1 + M_2 + (n + l) \log_2 d_2 \right) \left(d^m d_1 \right)^{O(1)}.$$

ii) L'algorithme calcule une famille de polynômes homogènes $\psi_1, \dots, \psi_N \in F[X_0, \dots, X_n]$ qui définit W , i.e.,

$$W = V(\psi_1, \dots, \psi_N) \subset P^n(\overline{F})$$

avec les bornes suivantes :

- $N \leq m^2 d^{4m}$.

- $\deg_{X_0, \dots, X_n}(\psi) \leq d^{2m}$, $\deg_{T_1, \dots, T_l}(\psi_i) \leq d_2(d^m d_1)^{O(1)}$.

- La taille binaire de coefficients de ψ_i est donnée par

$$l(\psi_i) \leq \left(M_1 + M_2 + l \log_2 d_2 \right) \left(d^m d_1 \right)^{O(1)}.$$

La complexité binaire totale de ce calcul est bornée par

$$(pkM_1M_2)^{O(1)}(d^n d_1 d_2)^{O(c+l)}$$

où $c = 1 + \max \dim(W) \leq 1 + n$. Donc pour p, M_1, M_2, d_1, d_2, l fixés, cette complexité est polynomiale en d^{n^2} .

iii) L'algorithme représente chaque composante absolument irréductible W_1 de W par un point générique *efficace* et par une famille finie de polynômes qui la définit avec les mêmes bornes sur les degrés et les tailles binaires de polynômes intermédiaires comme dans i) et ii). L'algorithme calcule une extension séparable maximale $F(c)$ de F là où W_1 est définie et irréductible avec le polynôme minimal $\chi \in F[C]$ de c sur F qui vérifie :

- $\deg_C(\chi) \leq \deg W_1$, $\deg_{T_1, \dots, T_l}(\chi) \leq d_2(d^m d_1)^{O(1)}$.

- La taille binaire de coefficients de χ est donnée par

$$l(\chi) \leq \left(M_1 + M_2 + (n + l) \log_2 d_2 \right) \left(d^m d_1 \right)^{O(1)}.$$

La complexité binaire totale de cette construction est égale à celle de i) et ii).

Cet algorithme est basé sur un algorithme polynomial de factorisation de polynômes multivariés sur le corps F décrit dans [25, 23, 22, 58]. L'idée de représenter les composantes irréductibles d'une telle façon vient du cas $k = 1$, i.e., la variété $V = V(f_1)$ est une hypersurface de $P^n(\overline{F})$. Dans ce cas si on factorise f_1 en produit de facteurs

irréductibles g_1, \dots, g_s sur F alors les composantes irréductibles de V sont les hypersurfaces $V(g_i)$, $1 \leq i \leq s$ définis par les polynômes g_1, \dots, g_s . Prenons un certain g_i et l'écrivons comme un polynôme univarié en X_n , i.e.,

$$g_i = \tilde{g}_i(X_0^{p^\nu}, \dots, X_n^{p^\nu}) = A_h X_n^h + \dots + A_1 X_n + A_0$$

où $h = \deg_{X_n}(g_i)$, $0 \neq A_h, \dots, A_1, A_0 \in F[X_0, \dots, X_{n-1}]$ et p^ν est la puissance maximale qu'on peut extraire. Posons $t_1 = \frac{X_1}{X_0}, \dots, t_{n-1} = \frac{X_{n-1}}{X_0}$, une représentation paramétrique des éléments de $V(g_i)$ est donnée par

$$\Phi(t_1, \dots, t_{n-1}, \theta) = 0, \quad \begin{cases} \frac{X_1}{X_0} & = t_1 \\ \vdots & \\ \frac{X_{n-1}}{X_0} & = t_{n-1} \\ \left(\frac{X_n}{X_0}\right)^{p^\nu} & = \theta \end{cases}$$

où θ est algébrique sur $F(t_1, \dots, t_{n-1})$ de polynôme minimal

$$\Phi(Z) = \frac{\tilde{g}_i(t_1, \dots, t_{n-1}, Z)}{A_h(t_1, \dots, t_{n-1})} \in F(t_1, \dots, t_{n-1})[Z]$$

($\tilde{g}_i \in F[Z_0, \dots, Z_n]$ est irréductible sur F où Z_0, \dots, Z_n sont de nouvelles variables).

2.3 Elimination de quantificateurs dans la théorie des corps algébriquement clos

Cette section est divisée en trois paragraphes. Nous décrivons dans le premier paragraphe le problème d'élimination de quantificateurs dans la théorie des corps algébriquement clos. On passe dans le deuxième à l'histoire de ce sujet avec les meilleures bornes de complexité des algorithmes qui le résolvent. Dans le troisième paragraphe, on détaille l'algorithme de Chistov-Grigoriev décrit en 1984.

2.3.1 Description du problème

Une formule est une collection des atomes avec les symboles des connections \vee (ou), \wedge (et), \neg (négation) et les quantificateurs \exists et \forall . Un atome est de la forme $P = 0$ ou $P \neq 0$, où P est un polynôme de $F[X_1, \dots, X_n]$. Pour une formule ϕ , il y a deux sortes des variables, les variables liées (ou quantifiée) et les variables libres (ou non-quantifiée). On note $lib(\phi)$, l'ensemble des variables libres de ϕ , cet ensemble vérifie les propriétés suivantes :

- Un atome $P = 0$ ou $P \neq 0$, où $P \in F[X_1, \dots, X_n]$ est une formule avec variables libres X_1, \dots, X_n .

- Si ϕ_1 et ϕ_2 sont deux formules alors $\phi_1 \vee \phi_2$ et $\phi_1 \wedge \phi_2$ sont aussi de formules et $lib(\phi_1 \vee \phi_2) = lib(\phi_1 \wedge \phi_2) = lib(\phi_1) \cup lib(\phi_2)$.
- Si ϕ est une formule alors $\neg\phi$ est une formule avec $lib(\neg\phi) = lib(\phi)$.
- Si ϕ est une formule et $X \in lib(\phi)$ alors $(\exists X)\phi$ et $(\forall X)\phi$ sont aussi de formules avec $lib((\exists X)\phi) = lib((\forall X)\phi) = lib(\phi) \setminus \{X\}$

Une formule est dite non-quantifiée si elle ne contient pas de quantificateurs. Une formule ϕ sans variables libres, i.e., $lib(\phi) = \emptyset$ est appelée sentence.

D'une manière générale, on peut représenter une formule ϕ à coefficients dans F avec variables libres u_1, \dots, u_r par :

$$\phi := \phi(u_1, \dots, u_r) := (Q_1 X_1) \cdots (Q_n X_n) \mathcal{F}(X_1, \dots, X_n, u_1, \dots, u_r)$$

où $Q_i \in \{\exists, \forall\}$ et \mathcal{F} est une formule non-quantifiée qui contient des polynômes de $F[X_1, \dots, X_n, u_1, \dots, u_r]$. Celle-ci est appelée la forme normale prenex de ϕ et X_1, \dots, X_n sont ses variables liées.

La \overline{F} -réalisation de ϕ , notée $\mathcal{R}(\phi, \overline{F}^r)$, est l'ensemble des $a = (a_1, \dots, a_r) \in \overline{F}^r$ tel que la sentence obtenue $\phi(a)$ est vérifiée, i.e.,

$$\mathcal{R}(\phi, \overline{F}^r) := \{a = (a_1, \dots, a_r) \in \overline{F}^r / \phi(a)\}.$$

Deux formules ϕ et ψ avec les mêmes variables libres u_1, \dots, u_r sont dites \overline{F} -équivalentes si $\mathcal{R}(\phi, \overline{F}^r) = \mathcal{R}(\psi, \overline{F}^r)$.

Exemple 2.3.1 *Considérons la formule suivante :*

$$\phi_1 := \phi_1(u_0, u_1, \dots, u_r) := (\exists X, u_r X^r + \cdots + u_1 X + u_0 = 0)$$

dont X est la seule variable liée et u_0, u_1, \dots, u_r sont ses variables libres.

La \mathbf{C} -réalisation $\mathcal{R}(\phi_1, \mathbf{C}^{r+1})$ est l'ensemble des uples $a = (a_0, a_1, \dots, a_r) \in \mathbf{C}^{r+1}$ tel que le polynôme univarié associé $P(X) = a_r X^r + \cdots + a_1 X + a_0$ admet une racine dans \mathbf{C} , ceci est toujours vérifié à moins que $P(X)$ est un polynôme constant non nul. Donc

$$\mathcal{R}(\phi_1, \mathbf{C}^{r+1}) = \{a \in \mathbf{C}^{r+1}, \bigvee_{1 \leq i \leq r} (a_i \neq 0) \vee (a_0 = 0)\}$$

En d'autre terme, la formule quantifiée ϕ_1 est \mathbf{C} -équivalente à la formule non-quantifiée ψ_1 qui est définie par :

$$\psi_1 := \psi_1(u_0, u_1, \dots, u_r) := \bigvee_{1 \leq i \leq r} (u_i \neq 0) \vee (u_0 = 0).$$

Exemple 2.3.2 Soit la formule

$$\phi_2 := (\exists X, u_r X^r + \cdots + u_1 X + u_0 \neq 0)$$

$\mathcal{R}(\phi_2, \mathbf{C}^{r+1})$ est l'ensemble des uples $a = (a_0, a_1, \dots, a_r) \in \mathbf{C}^{r+1}$ tel que le polynôme univarié associé n'est pas nul. Donc

$$\mathcal{R}(\phi_2, \mathbf{C}^{r+1}) = \{a \in \mathbf{C}^{r+1}, \forall_{0 \leq i \leq r} (a_i \neq 0)\}$$

et ϕ_2 est \mathbf{C} -équivalente à la formule non-quantifiée suivante :

$$\psi_2 := \forall_{0 \leq i \leq r} (u_i \neq 0).$$

Définition 2.3.3 Un ensemble constructible de \overline{F}^r , défini sur F , est la \overline{F} -réalisation d'une formule non-quantifiée à coefficients dans F

Le problème d'élimination de quantificateurs dans la théorie des corps algébriquement clos est l'un des problèmes essentiels de la théorie d'élimination et de la géométrie algébrique. Il s'agit d'éliminer les quantificateurs dans une formule quantifiée $\phi(u_1, \dots, u_r)$, i.e., calculer une formule non-quantifiée $\psi(u_1, \dots, u_r)$ qui est \overline{F} -équivalente à ϕ .

L'étude de ce problème se ramène à trouver des méthodes constructives efficaces qui calculent ψ . Par conséquence, étudier la complexité de ces algorithmes en tant que nombre d'opérations élémentaires dans le corps de base F .

2.3.2 Historique

Plusieurs algorithmes connus pour ce problème sont basés sur l'efficacité d'une procédure qui résout le problème de décision suivant : Décider si une famille de polynômes multivariés à coefficients dans F admet une solution algébrique commune dans \overline{F} . Géométriquement, ceci est équivalent au problème de décider si une variété algébrique est vide ou non, plus généralement, décider si un ensemble constructible est vide ou non.

Il est bien connu que par le théorème des zéros de Hilbert, ce problème de décision est équivalent à celui d'appartenance d'un polynôme à un idéal polynomial dont l'algèbre linéaire [93] et les bases de Gröbner [31] le résolvent.

D'autres algorithmes pour ce problème de décision utilisent la théorie des résultants pour éliminer les variables (si les polynômes sont homogènes) et le ramènent à tester si une certaine quantité (appelée résultant de la famille de polynômes) est nulle ou non (Voir [117, 93], la section précédante et le chapitre 3).

Notons que dans la théorie des corps réellement clos, l'élimination des quantificateurs d'une formule quantifiée avec atomes de la forme $P = 0, P > 0, P < 0$ où

$P \in F[X_1, \dots, X_n]$, ici F est un corps réellement clos, a été étudié par Tarski et Seidenberg en décrivant une procédure d'élimination des quantificateurs avec une complexité hyperexponentielle. Par une décomposition algébrique cylindrique, Collins [28] a décrit un algorithme d'élimination de quantificateurs sur les réels avec une complexité doublement exponentielle de la forme :

$$(kd)^{O(1)^{n+r}}$$

où k est le nombre d'atomes et d est une borne supérieure de degrés des atomes dans la formule ϕ étudiée.

D'autres algorithmes avec le même genre de complexité ont été fait par Ben-Or, Kozen et Reif [9], Weispfenning [123], Davenport et Heintz [34] (pour une borne inférieure).

Le problème de décision dans le cas réel se fait dans un temps simplement exponentiel en n (voir [63, 62, 16]) et dans un temps doublement exponentielle en le nombre d'alternance de quantificateurs dans la formule étudiée, i.e., de la forme :

$$(kd)^{O(n+r)^{4m-2}}$$

où m est le nombre d'alternance de quantificateurs [63]. Heintz et. al. [68] et Renegar [106] ont montré que le problème d'élimination de quantificateurs par bloc se fait avec des algorithmes bien parallélisables de complexités doublement exponentielles en m . Nous n'abordons pas le cas réellement clos dans la suite de cette section et nous nous intéressons seulement au cas algébriquement clos.

Une borne de complexité doublement exponentielle en n a été établi par Heintz dans [66] pour l'élimination des quantificateurs dans la théorie des corps algébriquement clos. La première borne simplement exponentielle en n et doublement exponentielle en m est réalisée dans les travaux de Chistov et Grigoriev [24], i.e., de la forme

$$(kd)^{O(n+r)^{2m+2}}.$$

Nous détaillons au paragraphe suivant leur algorithme qui sera utilisé tout au long de prochains chapitres surtout les bornes sur les degrés et les tailles de polynômes obtenus qui définissent la formule non-quantifiée. Cet algorithme est parallélisable si le caractéristique de F est positif et n'est pas parallélisable si le caractéristique de F est zéro car il utilise l'algorithme LLL de [89] pour calculer un vecteur minimal.

Fitchas, Galligo et Morgenstern [40] ont décrit un algorithme bien parallélisable avec une complexité séquentielle simplement exponentielle en n . En 1998, Puddu et Sabia [104] décrivent un algorithme bien parallélisable d'élimination de quantificateurs avec une complexité séquentielle

$$(kd)^{O(n+r)^m}$$

simplement exponentielle en n et doublement exponentielle en m , la sortie de cet algorithme est représentée par un programme d'évaluation.

2.3.3 Algorithme de Chistov-Grigoriev

Cet algorithme [24] élimine les quantificateurs d'une formule définie sur une large classe de corps, i.e., le corps $F = H(T_1, \dots, T_l)[\eta]$ introduit au chapitre 1. Il est basé sur leur algorithme de factorisation de polynômes multivariés à coefficients dans F d'une part et sur leur algorithme de décomposition d'une variété algébrique en composantes irréductibles [23, 22, 58] d'autre part. Nous montrons ici l'entrée, la sortie, la complexité binaire totale de cet algorithme ainsi que les bornes sur les degrés et les tailles de polynômes de la sortie.

Considérons la formule quantifiée suivante :

$$\Phi(u_1, \dots, u_r) := (\exists X_1) \cdots (\exists X_n) (\wedge_{1 \leq i \leq k} f_i = 0 \wedge g \neq 0)$$

où $f_i, g \in F[u_1, \dots, u_r, X_1, \dots, X_n]$, de degrés bornés par d (resp. δ) par rapport à X_1, \dots, X_n (resp. u_1, \dots, u_r), les variables u_1, \dots, u_r sont les variables libres de Φ . Ces polynômes sont donnés en représentation dense par leurs vecteurs de coefficients dans H , leurs bornes sur les degrés par rapport à T_1, \dots, T_l ainsi que leurs tailles binaires de coefficients dans H sont comme dans le chapitre 1.

L'algorithme construit une formule non-quantifiée $\Psi(u_1, \dots, u_r)$, qui est \overline{F} -équivalente à $\Phi(u_1, \dots, u_r)$ et définie par

$$\Psi(u_1, \dots, u_r) := \bigvee_{1 \leq i \leq \alpha} \left(\bigwedge_{1 \leq j \leq \beta} (B_j^{(i)} = 0) \wedge (C^{(i)} \neq 0) \right)$$

avec pour tout $1 \leq i \leq \alpha$ et $1 \leq j \leq \beta$ on a :

- 1) $B_j^{(i)}, C^{(i)} \in F[u_1, \dots, u_r]$.
- 2) $\deg_{u_1, \dots, u_r}(B_j^{(i)}) \leq \delta(kd)^{4(n+r+2)(2n+3)}$.
- 3) $\deg_{u_1, \dots, u_r}(C^{(i)}) \leq \delta(3kd)^{2n+3}$.
- 4) $\deg_{T_1, \dots, T_l}(B_j^{(i)}) \leq \delta d_2 d_1^{O(1)} (kd)^{O(n^2 r)}$.
- 5) $\deg_{T_1, \dots, T_l}(C^{(i)}) \leq \delta d_2 d_1^{O(1)} (kd)^{O(n)}$.
- 6) $l(B_j^{(i)}) \leq \left(M_1 + M_2 + (n + r + l) \log_2 d_2 \right) \delta d_1^{O(1)} (kd)^{O(n^2 r)}$.
- 7) $l(C^{(i)}) \leq \left(M_1 + M_2 + (n + r + l) \log_2 d_2 \right) \delta d_1^{O(1)} (kd)^{O(n)}$.
- 8) $\alpha, \beta \leq \delta(kd)^{O(n^2 r)}$.

La complexité binaire totale de cet algorithme est

$$(p\delta M_1 M_2)^{O(1)} (d_1 d_2)^{O(n+r+l)} (kd)^{O(n(n+r)(n+r+l))}.$$

Si la formule Φ est définie par m blocs de quantificateurs, i.e., de la forme

$$\Phi(u_1, \dots, u_r) := \exists(X_{1,1}, \dots, X_{1,s_1}) \forall(X_{2,1}, \dots, X_{2,s_2}) \cdots \exists(X_{m,1}, \dots, X_{m,s_m}) \mathcal{F}$$

où \mathcal{F} est formule non-quantifiée avec k atomes dans $F[u_1, \dots, u_r, X_{1,1}, \dots, X_{m,s_m}]$.

L'itération m fois de l'algorithme précédent sur la formule Φ conduit à une formule non-quantifiée \bar{F} équivalente à Φ définie par des atomes $h \in F[u_1, \dots, u_r]$ vérifiant :

- 1) $\deg_{u_1, \dots, u_r}(h) \leq \delta(kd^s)^{O(s^2 m)^m}$.
- 2) $\deg_{T_1, \dots, T_l}(h) \leq \delta d_2 d_1^{O(m)} (kd^s)^{O(s^2 m)^m}$.
- 3) $l(h) \leq (M_1 + M_2 + l \log_2 d_2) d_1^{O(m)} (kd^s)^{O(s^2 m)^m}$.
- 4) Le nombre des atomes h est borné par $\delta(kd^s)^{O(s^2 m)^m}$.

La complexité binaire totale de cet algorithme est

$$(p\delta M_1 M_2)^{O(1)} (d_1^m d_2)^{O(s+l)} (kd^s)^{O(s^3 l)^m}$$

où $s := r + s_1 + \dots + s_m$ est le nombre total de variables.

2.4 Résolution des systèmes linéaires paramétriques

Considérons le système linéaire

$$AX = b$$

où $A = (A_{ij})_{1 \leq i, j \leq n}$ est une matrice carrée d'ordre n et $b = (b_i)_{1 \leq i \leq n}$ est un vecteur. Les entrées $A_{i,j}$ et b_i ($1 \leq i, j \leq n$) appartiennent à l'anneau polynomial $F[u_1, \dots, u_r]$ de degrés bornés par δ . Les variables (u_1, \dots, u_r) sont de paramètres qui prennent des valeurs dans l'espace \bar{F}^r qui sera appelé l'espace des paramètres. Le système $AX = b$ est ainsi appelé un système linéaire paramétré. Nous allons étudier dans ce paragraphe la dépendance de solutions de ce système en fonction de paramètres.

Il est bien connu qu'un système linéaire (non-paramétré) se trouve uniquement dans l'un de trois cas suivants : aucune solution, une seule solution, une infinité de solutions. L'ouvert de \bar{F}^r défini par $\det(A) \in F[u_1, \dots, u_r]$ est le lieu là où le système associé admet

une seule solution dans \overline{F}^n . Cette solution est donnée par les formules de Cramer comme une fonction rationnelle de paramètres :

$$X_j = \frac{\det(A_j)}{\det(A)} \in F(u_1, \dots, u_r) \quad 1 \leq j \leq n$$

où A_j est la matrice obtenue en remplaçant la j -ème colonne de A par le vecteur b .

On s'intéresse aussi au complémentaire de cet ouvert dans l'espace de paramètres i.e., là où la matrice A est non inversible. Nous avons cité au premier chapitre les travaux de Heintz [66] et de William Sit [114, 113] qui a décrit un algorithme qui décompose l'espace de paramètres en un nombre fini d'ensembles constructibles S deux à deux disjoints. Le rang de la matrice A est constant sur chaque S et une base de l'espace de solution du système homogène associé est donnée comme une fonction rationnelle de paramètres (évidemment l'un de ces ensembles constructibles est le lieu d'inconsistance du système). Le nombre de ces ensembles est exponentiel en n .

2.4.1 Algorithme de Gauss paramétrique

La paramétrisation de l'algorithme de Gauss consiste à performer l'algorithme de Gauss ordinaire et à séparer dans chaque étape le cas où le pivot de Gauss est nul ou non. Celui-ci est un élément de $F[u_1, \dots, u_r]$ et le fait qu'il est nul ou non définit un sous-ensemble constructible de l'espace des paramètres.

Le corps F considéré ici est le corps $H(T_1, \dots, T_l)[\eta]$ du premier chapitre. Les entrées $A_{i,j}$ et b_i ($1 \leq i, j \leq n$) sont données en représentation dense par leurs vecteurs de coefficients dans H . Leurs degrés par rapport à T_1, \dots, T_l sont bornés par d_2 et les tailles binaires de leurs coefficients dans H sont bornées par M_2 .

Cet algorithme construit donc une famille des couples $(C^{(i)}, A^{(i)})$, $0 \leq i \leq n$ où $C^{(0)} = \overline{F}^r$, $A^{(0)} = A$, $C^{(i)}$ ($1 \leq i \leq n$) est un sous-ensemble constructible de \overline{F}^r donné par ses équations et ses inéquations qui le définissent et $A^{(i)} = \left(A_{s,t}^{(i)} \right)_{1 \leq s,t \leq n}$ est une matrice à coefficients dans $F[u_1, \dots, u_r]$ obtenue à partir de A par transformations linéaires sur les lignes et par de permutations. Cette matrice est donnée par :

$$A^{(i)} = \begin{pmatrix} A_{1,1}^{(i)} & \dots & \dots & \dots & \dots & \dots & A_{1,n}^{(i)} \\ 0 & A_{2,2}^{(i)} & \dots & \dots & \dots & \dots & A_{2,n}^{(i)} \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & 0 & A_{i,i}^{(i)} & \dots & \dots & A_{i,n}^{(i)} \\ \vdots & \vdots & \vdots & 0 & A_{i+1,i+1}^{(i)} & \dots & A_{i+1,n}^{(i)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & A_{n,i+1}^{(i)} & \dots & A_{n,n}^{(i)} \end{pmatrix}$$

Pour tout $a \in C^{(i)}$

$$A_{1,1}^{(i)}(a) \neq 0, \dots, A_{i,i}^{(i)}(a) \neq 0.$$

Cette construction se fait par induction sur i . On suppose qu'à l'étape i , $C^{(i)}$ est défini par des équations et des inéquations de la forme $g = 0$ et $h \neq 0$ où $g, h \in F[u_1, \dots, u_r]$ qui vérifient :

- Les degrés de g, h et $A_{s,t}^{(i)}$ ($1 \leq s, t \leq n$) par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $i\delta$ (resp. id_2).

- Les tailles binaires de coefficients de g, h et $A_{s,t}^{(i)}$ ($1 \leq s, t \leq n$) sont bornées par

$$i(M_2 + 1)$$

L'étape $i + 1$ consiste à faire les démarches suivantes :

- Si $A_{i+1,i+1}^{(i)} \in F[u_1, \dots, u_r]$ est linéairement dépendant des polynômes g , échanger la $(i + 1)$ -ème ligne de $A^{(i)}$ par la $(i + 2)$ -ème ligne et tester de nouveau si $A_{i+2,i+1}^{(i)}$ est linéairement dépendant des éléments g et ainsi de suite. Chaque test correspond à résoudre un certain système linéaire d'au plus i inconnues et $\binom{r+i\delta}{r} \leq (i\delta)^r$ équations à coefficients dans F . Cette résolution se fait avec $(i\delta)^{O(r)}$ opérations dans F [95]. Chacune de ces opérations se fait entre deux éléments de degrés $\leq id_2$ par rapport à T_1, \dots, T_l et des tailles binaires $\leq i(M_2 + 1)$. Alors chaque test se fait avec

$$(i\delta d_1 d_2)^{O(rl)}$$

opérations dans le corps H . Sa complexité binaire est bornée par

$$M_1 M_2 (i\delta d_1 d_2)^{O(rl)}$$

- Si tous les $A_{s,t}^{(i)}$, $s \geq i+1$, $t \geq i+1$ (après des échanges des colonnes aussi) sont linéairement dépendants de polynômes g alors $A_{s,t}^{(i)}(a) = 0$ pour tout $a \in C^{(i)}$. Dans ce cas l'algorithme s'arrête et ne considère pas le couple $(C^{(i+1)}, A^{(i+1)})$. Le nombre des tests à effectuer ici est égale à $(n - i)^2$. Ces tests se font avec

$$n^2 (i\delta d_1 d_2)^{O(rl)}$$

opérations dans H et avec une complexité binaire bornée par

$$n^2 M_1 M_2 (i\delta d_1 d_2)^{O(rl)}$$

- S'il existe $s_0 \geq i + 1$, $t_0 \geq i + 1$ tel que $A_{s_0,t_0}^{(i)}$ est linéairement indépendant de polynômes

g alors on pose $C^{(i+1)} = C^{(i)} \cap \{A_{s_0, t_0}^{(i)} \neq 0\}$. Après échange des lignes et des colonnes, on met $A_{s_0, t_0}^{(i)}$ dans la position $(i+1, i+1)$ et on applique les transformations linéaires ordinaires sur les lignes $i+2, \dots, n$ sur la matrice obtenue qui rendent zéros les entrées au-dessous de $A_{s_0, t_0}^{(i)}$ ($A_{s_0, t_0}^{(i)}$ est le pivot de Gauss paramétrique, i.e., $A_{s_0, t_0}^{(i)}(a) \neq 0$ pour tout $a \in C^{(i+1)}$). Donc $A^{(i+1)}$ est la matrice obtenue vérifiant $A_{i+1, i+1}^{(i+1)} = A_{s_0, t_0}^{(i)}$ ne s'annule pas sur $C^{(i+1)}$.

Par la méthode de Bareiss (voir e.g., [14, 8]), les coefficients $A_{s, t}^{(i+1)} \in F[u_1, \dots, u_r]$ sont des $(i+1) \times (i+1)$ mineurs de la matrice A donnés par la formule :

$$A_{s, t}^{(i+1)} = \det \begin{pmatrix} A_{1,1} & \dots & A_{1,i} & A_{1,t} \\ \vdots & & \vdots & \vdots \\ A_{i,1} & \dots & A_{i,i} & A_{i,t} \\ A_{s,1} & \dots & A_{s,i} & A_{s,t} \end{pmatrix}$$

ce qui prouve les bornes de récurrence ci-dessus sur la taille binaire et les degrés de $A_{s, t}^{(i+1)}$ par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l .

Puisque le nombre d'étapes est au plus n alors la complexité totale de l'algorithme de Gauss paramétrique est

$$(n\delta d_1 d_2)^{O(rl)}$$

opérations dans H . Sa complexité binaire totale est

$$M_1 M_2 (n\delta d_1 d_2)^{O(rl)}.$$

Cette borne de complexité est polynomiale en la taille n de la matrice A et le degré δ des entrées de A par rapport aux paramètres. Elle est exponentielle en le nombre r des paramètres. On peut résumer cette section par le théorème suivant :

Théorème 2.4.1 *Il existe un algorithme, appelé l'algorithme de Gauss paramétrique qui pour un système linéaire paramétré $AX = b$ vérifiant les conditions ci-dessus, produit une partition de l'espace des paramètres \overline{F}^r sous la forme :*

$$\overline{F}^r = \bigcup_{0 \leq i \leq n} \mathcal{U}_i$$

où chaque \mathcal{U}_i est un ensemble constructible vérifiant :

- a) Le rang de A est constant sur \mathcal{U}_i et est égale à i , i.e., pour tout $a \in \mathcal{U}_i$, $\text{rg}(A(a)) = i$.
- b) L'algorithme calcule $(n - i + 1)$ vecteurs Z_0, Z_1, \dots, Z_{n-i} de $F(u_1, \dots, u_r)^n$ où Z_0 est une solution particulière paramétrique du système $AX = b$ et $\{Z_1, \dots, Z_{n-i}\}$ est une base paramétrique de l'espace de solutions de dimension $n - i$ du système paramétré

homogène, i.e., pour tout $a \in \mathcal{U}_i$ on a :

i) Les dénominateurs des entrées de Z_0, Z_1, \dots, Z_{n-i} ne s'annulent pas en a .

ii) $Z_0^{(a)}$ est une solution particulière du système spécialisé en a (i.e., le système $A^{(a)}X = b^{(a)}$) et la famille $\{Z_1^{(a)}, \dots, Z_{n-i}^{(a)}\}$ forme une base du système homogène associé.

c) Les degrés des équations et des inéquations qui définissent \mathcal{U}_i et des entrées de Z_0, Z_1, \dots, Z_{n-i} par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $n\delta$ (resp. nd_2). Leurs tailles binaires sont bornées par

$$nM_2.$$

d) La complexité de cet algorithme est celle qui est donnée juste au-dessus du théorème.

2.5 Calcul d'un P.G.C.D. d'une famille finie de polynômes univariés paramétrés

Considérons une famille finie $\{f_1, \dots, f_k\} \subset F[u_1, \dots, u_r, X]$ de polynômes paramétrés univariés, de degrés bornés par d (resp. δ et d_2) par rapport à X (resp. u_1, \dots, u_r et T_1, \dots, T_l). Ces polynômes sont donnés en représentation dense par leurs vecteurs de coefficients dans H , de tailles binaires bornées par M_2 . On s'intéresse dans ce paragraphe au calcul d'un p.g.c.d. de la famille $\{f_1^{(a)}, \dots, f_k^{(a)}\} \subset \overline{F}[X]$ d'une manière uniforme pour toute spécialisation $a = (a_1, \dots, a_r)$ des paramètres dans l'espace des paramètres \overline{F}^r où $f_i^{(a)} := f_i(a_1, \dots, a_r, X)$ pour tout $1 \leq i \leq k$.

Ecrivons chaque f_i ($1 \leq i \leq k$) sous la forme :

$$f_i = \sum_{0 \leq j \leq d} f_{ij} X^j \quad \text{où } f_{ij} \in F[u_1, \dots, u_r], \deg(f_{ij}) \leq \delta.$$

On s'intéresse à l'ouvert

$$U = \overline{F}^r \setminus V(f_{ij}, 1 \leq i \leq k, 0 \leq j \leq d)$$

de \overline{F}^r pour la topologie de Zariski.

On présente dans cette section trois algorithmes qui calculent un p.g.c.d. de la famille $\{f_1^{(a)}, \dots, f_k^{(a)}\} \subset \overline{F}[X]$ d'une manière uniforme pour toute spécialisation $a \in U$. Le premier algorithme est exponentiel en k et d et basé sur l'algorithme d'Euclide. Le deuxième et le troisième algorithme sont polynomiaux en k, d et exponentiels en r . Le troisième est basé sur la résolution des systèmes linéaires paramétrés de la section précédente.

2.5.1 Algorithme A1

Supposons que $k = 2$ et considérons f_1, f_2 comme de polynômes univariés à coefficients dans le corps $F(u_1, \dots, u_r)$ de fonctions rationnelles en les paramètres. Calculons la séquence

$$(R_0, R_1, \dots, R_s, R_{s+1} = 0) \subset F(u_1, \dots, u_r)[X]$$

des restes de divisions euclidiennes successives appliquées sur $R_0 := f_1$ et $R_1 := f_2$, i.e., pour tout $2 \leq i \leq s+1$, R_i est le reste de la division euclidienne de R_{i-2} par R_{i-1} . Cette séquence ne couvre pas les p.g.c.d. de $f_1^{(a)}, f_2^{(a)}$ pour toutes les spécialisations $a \in U$ de paramètres pour les deux raisons suivantes :

- 1) Les zéros des dénominateurs des coefficients de R_0, R_1, \dots, R_s ne sont pas couverts.
- 2) Pour tout $a \in U$ qui n'annule aucun dénominateur de coefficients de R_2, \dots, R_s , $R_s^{(a)} \in \overline{F}[X]$ n'est pas nécessairement un p.g.c.d. de $f_1^{(a)}$ et $f_2^{(a)}$ même s'il est non nul. Tandis que R_s est un p.g.c.d. de f_1 et f_2 dans $F(u_1, \dots, u_r)[X]$.

Le premier problème peut-être éviter par un calcul des séquences de pseudo-restes de divisions euclidiennes successives :

Définition 2.5.1 Soient $g, h \in F[u_1, \dots, u_r][X]$ deux polynômes univariés.

a) La pseudo-division de g par h est la division euclidienne de $lc(h)^{\deg(g)-\deg(h)+1}g$ par h dans $F(u_1, \dots, u_r)[X]$ où $0 \neq lc(h) \in F[u_1, \dots, u_r]$ est le coefficient dominant de h . Alors ils existent de polynômes uniques $Q, R \in F[u_1, \dots, u_r][X]$ tel que

$$lc(h)^{\deg(g)-\deg(h)+1}g = Qh + R \quad \text{avec} \quad \deg_X(R) < \deg_X(h)$$

Q est appelé le pseudo-quotient et R est le pseudo-reste de la pseudo-division de g par h , noté $\text{Prem}(g, h)$.

b) La séquence de pseudo-restes de pseudo-divisions successives appliquées à $\tilde{R}_0 := g$ et $\tilde{R}_1 := h$ est la séquence

$$(\tilde{R}_0, \tilde{R}_1, \dots, \tilde{R}_s, \tilde{R}_{s+1} = 0)$$

où pour tout $2 \leq i \leq s+1$, \tilde{R}_i est le pseudo-reste de la pseudo-division de \tilde{R}_{i-2} par \tilde{R}_{i-1} .

Le lemme suivant nous montre que la séquence de pseudo-restes permet aussi de calculer le p.g.c.d. et nous donne les bornes sur les degrés et les tailles binaires des polynômes qui constituent la séquence :

Lemme 2.5.2 Soient $g, h \in F[u_1, \dots, u_r][X]$ deux polynômes univariés de degrés $\leq d$ où F est le corps $H(T_1, \dots, T_l)[\eta]$. On suppose que les degrés de g et h par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par δ (resp. d_2), leurs tailles binaires sont

$\leq M_2$. Soit $(\tilde{R}_0, \tilde{R}_1, \dots, \tilde{R}_s, \tilde{R}_{s+1} = 0)$ la séquence de pseudo-restes de pseudo-divisions successives appliquées à $\tilde{R}_0 := g$ et $\tilde{R}_1 := h$. Alors

a) \tilde{R}_s est un p.g.c.d. de g et h dans $F[u_1, \dots, u_r][X]$. Pour tout $a \in U$ qui n'est pas zéro de tous les coefficients dominants de la séquence, $\tilde{R}_s^{(a)} \in \overline{F}[X]$ est un p.g.c.d. de $g^{(a)}$ et $h^{(a)}$.

b) Pour tout $0 \leq i \leq s$, le degré de \tilde{R}_i par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) est borné par $O(d^2\delta)$ (resp. $O(d^2d_2)$). La taille binaire de son vecteur de coefficients dans H est $\leq O(M_2 d^2 \log_2 d)$.

c) Le calcul de cette séquence se fait avec

$$O\left((\delta d_1 d_2)^2 d^9\right)$$

opérations dans H . Sa complexité binaire est

$$O\left((\delta d_1 d_2)^2 M_2^2 d^{13} \log_2^2 d\right).$$

Preuve. Toutes les bornes de ce lemme se déduisent des estimations de théorèmes 6.54, 6.62 et de l'exercice 6.54 de [118]. \square

Le deuxième problème peut-être évité par la considération de troncations :

Définition 2.5.3 Soit $g = g_m X^m + \dots + g_0 \in F[u_1, \dots, u_r][X]$ où $m := \deg(g)$.

a) Pour tout $0 \leq i \leq m$, la i -ème troncation de g , notée $Tro_i(g)$, est le polynôme

$$Tro_i(g) := g_i X^i + \dots + g_0 \in F[u_1, \dots, u_r][X]$$

b) L'ensemble de troncations de g , noté $Tro(g)$, est un sous-ensemble fini de $F[u_1, \dots, u_r][X]$ défini par

$$Tro(g) := \begin{cases} \{g\} & \text{si } g_m := lc(g) \in F \\ \{g\} \cup Tro(Tro_{m-1}(g)) & \text{sinon} \end{cases}$$

Définition 2.5.4 [8] Pour chaque polynôme $R \in Tro(f_1)$, on associe un arbre de séquences de pseudo-restes de divisions de f_1 par f_2 , noté $TRems(f_1, f_2)$, qui a R comme racine. Les fils de R sont les éléments de l'ensemble de troncations de f_2 . Chaque noeud N contient un polynôme $Pol(N) \in F[u_1, \dots, u_r][X]$. Un noeud N est une feuille de l'arbre si $Pol(N) = 0$. Si N n'est pas une feuille, les fils de N sont les éléments de l'ensemble de troncations de $Prem(Pol(p(N)), Pol(N))$ où $p(N)$ est le père de N . L'ensemble de tous les arbres associés aux éléments de $Tro(f_1)$ est appelé la forêt de séquences de pseudo-restes de divisions de f_1 par f_2 , elle est notée par $T(f_1, f_2)$.

Remarque 2.5.5 Chaque arbre $T\text{Rems}(f_1, f_2)$ dans la définition 2.5.4 se termine puisque le passage d'un niveau à un autre dans l'arbre se fait par une pseudo-division et donc par une diminution de degrés par rapport à X . Donc nous avons un nombre fini de feuilles dans l'arbre.

Définition 2.5.6 Soient $R_0 \in \text{Tro}(f_1)$ et $T\text{Rems}(f_1, f_2)$ l'arbre de racine R_0 . A chaque feuille L de $T\text{Rems}(f_1, f_2)$, on considère l'unique chemin $C_L := \{R_0, R_1, \dots, R_s, R_{s+1} := \text{Pol}(L) = 0\}$ liant L à la racine R_0 où $R_1 \in \text{Tro}(f_2)$ est un fils de R_0 et on associe à L un sous-ensemble constructible U_L de \overline{F}^r défini par la formule non-quantifiée suivante :

$$\bigwedge_{2 \leq i \leq s+1} \deg_X(R_i) = \deg_X(\text{Prem}(R_{i-2}, R_{i-1}))$$

Théorème 2.5.7 Les ensembles constructibles $\mathcal{U}_L := U_L \cap U$ où L sont les feuilles de la forêt $T(f_1, f_2)$ forment une partition de l'ouvert U . Cette partition vérifie les propriétés suivantes :

- a) Le nombre de feuilles L de $T(f_1, f_2)$ est borné par d^d .
- b) Les degrés des équations et des inéquations qui définissent chaque \mathcal{U}_L par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $O(d^2\delta)$ (resp. $O(d^2d_2)$). Leurs tailles binaires sont bornées par $O(M_2d^2 \log_2 d)$.
- c) Pour toute feuille L de $T(f_1, f_2)$, le chemin $C_L := \{R_0, R_1, \dots, R_s, R_{s+1} := \text{Pol}(L) = 0\}$ (voir définition 2.5.6) constitue une séquence paramétrée de pseudo-restes de f_1 et f_2 , i.e., pour tout $a \in \mathcal{U}_L$, la séquence $(R_0^{(a)}, R_1^{(a)}, \dots, R_s^{(a)}, R_{s+1} := \text{Pol}(L) = 0) \subset \overline{F}[X]$ est la séquence de pseudo-restes de $f_1^{(a)}$ et $f_2^{(a)}$. En particulier, $0 \neq R_s^{(a)} \in \overline{F}[X]$ est un p.g.c.d. de $f_1^{(a)}$ et $f_2^{(a)}$. Les degrés et la taille binaire de R_s sont analogues à ceux du point b) ci-dessus.
- d) La construction de la forêt $T(f_1, f_2)$ se fait avec

$$(\delta d_1 d_2)^2 d^{O(d)}$$

opérations dans H . Sa complexité binaire est

$$(\delta d_1 d_2 M_2)^2 d^{O(d)}.$$

Preuve. Toutes ces bornes se déduisent du lemme 2.5.2 ci-dessus. \square

Revenons maintenant au cas général, i.e., $k \geq 2$ et calculons une partition de U en un nombre fini d'ensembles constructibles chacun avec un p.g.c.d. paramétrique.

Théorème 2.5.8 Soient $f_1, \dots, f_k \in F[u_1, \dots, u_r][X]$ de polynômes paramétrés vérifiant les mêmes bornes ci-dessus sur les degrés et les tailles binaires de leurs coefficients. On peut construire une partition de l'ouvert U de \overline{F}^r en

$$d^{(k-1)d}$$

ensembles constructibles \mathcal{U} qui vérifient :

a) Les degrés des équations et des inéquations qui définissent chaque \mathcal{U} par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $O(d^{(2k-2)}\delta)$ (resp. $O(d^{(2k-2)}d_2)$). Leurs tailles binaires sont bornées par $O(M_2 d^{(2k-2)} \log_2^{k-1} d)$.

b) Pour tout ensemble constructible \mathcal{U} , il existe un polynôme $g \in F[u_1, \dots, u_r][X]$ tel que pour tout $a \in \mathcal{U}$, $g^{(a)} \in \overline{F}[X]$ est un p.g.c.d. de $f_1^{(a)}, \dots, f_k^{(a)}$. Les degrés et la taille binaire de g sont analogues à ceux du point a).

c) La construction de cette partition de U se fait avec

$$(\delta d_1 d_2)^2 d^{O(kd)}$$

opérations dans H . Sa complexité binaire est

$$(\delta d_1 d_2 M_2)^2 d^{O(kd)}.$$

Preuve. La démonstration se fait par induction sur k , le cas $k = 2$ est le théorème 2.5.7. Supposons qu'à l'étape $k - 1$ nous avons une partition de U en $d^{(k-2)d}$ ensembles constructibles \mathcal{V} chacun avec un polynôme paramétrique $G \in F[u_1, \dots, u_r][X]$ vérifiant les points a) et b) du théorème (pour f_1, \dots, f_{k-1}). Pour chaque couple (\mathcal{V}, G) , on calcule la forêt $T(G, f_k)$ et pour chaque feuille L de cette forêt, on considère l'ensemble constructible

$$\mathcal{V}_L := \mathcal{V} \cap U_L$$

où U_L est l'ensemble constructible associé à L dans $T(G, f_k)$ (voir définition 2.5.6). Les ensembles \mathcal{V}_L où L sont les feuilles de $T(G, f_k)$ pour tous les couples (\mathcal{V}, G) de l'étape $k - 1$, forment une partition de U . Pour chaque \mathcal{V}_L , le polynôme $g := \text{Pol}(p(L)) \in F[u_1, \dots, u_r][X]$ vérifie le point b). Les bornes sur les degrés et les tailles binaires de a) et b) ainsi la complexité totale se déduisent du théorème 2.5.7. \square

2.5.2 Algorithme A2

En 1989, Grigoriev [59] décrit un algorithme qui calcule un p.g.c.d. paramétrique de la famille $\{f_1, \dots, f_k\}$. Cet algorithme décompose U en

$$N_1 \leq k(\delta + d)^{O(r)}$$

ensembles constructibles \mathcal{U} qui vérifient :

i) Les degrés des équations et des inéquations qui définissent \mathcal{U} par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par

$$(\delta + d)^{O(1)}$$

(resp. $d_2(d_1(\delta + d))^{O(1)}$). Leur nombre est borné par $k(\delta + d)^{O(r)}$ et les tailles binaires de leurs coefficients dans H sont bornées par

$$\left(M_1 + M_2 + (l + r) \log_2(d_2) \right) \left(d_1(\delta + d) \right)^{O(1)}$$

ii) Pour chaque \mathcal{U} , l'algorithme calcule un polynôme paramétrique $g \in F[u_1, \dots, u_r, X]$ qui vérifie :

- $\deg_{u_1, \dots, u_r, X}(g) \leq (\delta + d)^{O(1)}, \deg_{T_1, \dots, T_l}(g) \leq d_2 \left(d_1(\delta + d) \right)^{O(1)}$.
- $l(g) \leq \left(M_1 + M_2 + (l + r) \log_2(d_2) \right) \left(d_1(\delta + d) \right)^{O(1)}$.
- Pour tout $a \in \mathcal{U}$, le polynôme $g^{(a)} \in \overline{F}[X]$ coïncide avec le p.g.c.d. de la famille $\{f_1^{(a)}, \dots, f_k^{(a)}\} \subset \overline{F}[X]$.

La complexité binaire totale de cet algorithme est

$$(kM_1M_2)^{O(1)}(d_1d_2)^{O(l)}(\delta + d)^{O(r+l)}.$$

2.5.3 Algorithme A3

L'idée de cet algorithme vient du lemme suivant :

Lemme 2.5.9 Soit $h_1, \dots, h_k \in F[X]$ de degrés $\leq d$ et $h = \text{pgcd}(h_1, \dots, h_k)$. Alors

a) Il existe de polynômes $g_1, \dots, g_k \in F[X]$ de degrés $< d$ tel que

$$h = \sum_{1 \leq i \leq k} g_i h_i$$

b) Le degré de h est donné par

$$\begin{aligned} D &:= \deg(h) \\ &= \min\{\deg(g); \exists g_1, \dots, g_k \in F[X], \deg(g_i) < d, \forall 1 \leq i \leq k, g = \sum_{1 \leq i \leq k} g_i h_i \neq 0\} \end{aligned}$$

Pour tout $0 \leq t \leq d$, on considère le système linéaire paramétré S_t défini par la propriété suivante :

$$\sum_{1 \leq i \leq k} g_i f_i \text{ est un polynôme unitaire de degré } t \text{ avec } \deg(g_i) < d.$$

Ecrivons chaque g_i sous la forme :

$$g_i = \sum_{0 \leq j < d} g_{ij} X^j$$

Alors S_t est défini par les équations linéaires paramétrées suivantes :

$$\sum_{1 \leq i \leq k, 0 \leq j \leq s} g_{ij} f_{i,s-j} = \begin{cases} 0 & Si \quad t < s < 2d \\ 1 & Si \quad s = t \end{cases}$$

Les inconnus de ce système sont les variables g_{ij} , leur nombre est kd , le nombre d'équations est $2d - t$. Les degrés des entrées du système S_t par rapport aux paramètres u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par δ (resp. d_2), leurs tailles binaires sont bornées par M_2 .

Appliquons l'algorithme de résolution des systèmes linéaires paramétrés de la section précédente sur les systèmes S_0, \dots, S_d , ceci nous permet de calculer de sous-ensembles constructibles $\mathcal{U}_0, \dots, \mathcal{U}_d$ de U avec de fonctions rationnelles

$$g_{0,i,j}, \dots, g_{d,i,j} \in F(u_1, \dots, u_r), \quad 1 \leq i \leq k, 0 \leq j < d.$$

qui vérifient :

i) $\mathcal{U} = \bigcup_{0 \leq t \leq d} \tilde{\mathcal{U}}_t$ où $\tilde{\mathcal{U}}_t := \mathcal{U}_t \setminus \bigcup_{0 \leq t' < t} \mathcal{U}_{t'}$.

ii) Pour tout $0 \leq t \leq d$, \mathcal{U}_t est le lieu de consistance du système S_t , i.e., pour tout $a \in \mathcal{U}_t$, le système S_t spécialisé en a admet le vecteur

$$\left(g_{t,i,j}^{(a)} \right)_{1 \leq i \leq k, 0 \leq j < d} \in \overline{F}^{kd}$$

comme solution particulière. Donc pour tout $a \in \tilde{\mathcal{U}}_t$ le polynôme unitaire $g_t^{(a)} \in \overline{F}[X]$ de degré t , coïncide avec le p.g.c.d. de $f_1^{(a)}, \dots, f_k^{(a)} \in \overline{F}[X]$ où

$$g_t = \sum_{1 \leq i \leq k, 0 \leq j < d} g_{t,i,j} X^j f_i \in F(u_1, \dots, u_r)[X]$$

iii) Les degrés des équations et des inéquations qui définissent chaque $\tilde{\mathcal{U}}_t$ ainsi de g_t ($0 \leq t \leq d$) par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $kd\delta$ (resp. kdd_2). Leurs tailles binaires sont bornées par kdM_2 .

De la complexité de l'algorithme de Gauss paramétrique (voir théorème 2.4.1), on déduit que cet algorithme se fait avec

$$(k\delta dd_1 d_2)^{O(rl)}$$

opérations dans H . Sa complexité binaire totale est

$$M_1 M_2 (k\delta dd_1 d_2)^{O(rl)}.$$

Chapitre 3

Résolution de systèmes algébriques paramétrés de dimensions zéros

3.1 Introduction et notations

Considérons k polynômes paramétrés $f_1, \dots, f_k \in F[u_1, \dots, u_r, X_0, \dots, X_n]$ homogènes en X_0, \dots, X_n , de degré $D_1, \dots, D_k \leq d$ respectivement. Le corps F est le corps $H(T_1, \dots, T_l)[\eta]$ introduit au chapitre 1 où $H = \mathbb{Q}$ si $\text{car}(F) = 0$ et $H \supset \mathbb{F}_p$ est un corps fini si $\text{car}(F) = p$. Chaque polynôme f_j ($1 \leq j \leq k$) est donné en représentation dense par ses coefficients dans H . On suppose que

$$\deg_{u_1, \dots, u_r} f_j \leq \delta, \deg_{T_1, \dots, T_l} f_j \leq d_2$$

La taille binaire de f_j est bornée par M_2 . On rappelle que M_1 est une borne supérieure de la taille binaire du polynôme minimal $\phi \in H(T_1, \dots, T_l)[Z]$ de η sur le corps $H(T_1, \dots, T_l)$ et que $\deg_{Z, T_1, \dots, T_l}(\phi) \leq d_1$.

Ces polynômes définissent un système algébrique paramétré $f_1 = \dots = f_k = 0$, les variables u_1, \dots, u_r sont les paramètres du système, leur nombre est borné par le nombre de coefficients de f_1, \dots, f_k , i.e., $r \leq kd^n$. Ces paramètres $u = (u_1, \dots, u_r)$ prennent de valeurs dans l'espace $\mathcal{P} := \overline{F}^r$ qui sera appelé comme d'habitude l'espace des paramètres.

Pour une certaine fonction rationnelle $g \in F(u_1, \dots, u_r)$, le degré de g par rapport à u_1, \dots, u_r est défini comme étant le maximum entre le degré de son numérateur et de son dénominateur par rapport à u_1, \dots, u_r (de la même manière on définit le degré de g par rapport à T_1, \dots, T_l). Pour tout $a \in \mathcal{P}$, $g^{(a)} \in \overline{F}$ est l'évaluation de g en a à condition que son dénominateur ne s'annule pas en a . On note $V^{(a)}$ la variété projective de $P^n(\overline{F})$ définie par les polynômes $f_1^{(a)}, \dots, f_k^{(a)} \in \overline{F}[X_0, \dots, X_n]$.

L'outil de base de ce chapitre est le calcul du résultant de chaque système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ ($a \in \mathcal{P}$) d'une manière uniforme sur les paramètres. On introduira ce qu'on appelle un U -résultant paramétrique où $U = (U_0, \dots, U_n)$ sont de nouvelles variables algébriquement indépendantes sur le corps $F(u_1, \dots, u_r, X_0, \dots, X_n)$. Chaque U -résultant paramétrique R est un polynôme de $F[u_1, \dots, u_r, U_0, \dots, U_n]$ homogène en U_0, \dots, U_n , associé à un sous-ensemble constructible W de \mathcal{P} tel que pour tout $a \in W$, $R^{(a)} \in \overline{F}[U_0, \dots, U_n]$ est le U -résultant du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ (voir les sections 1 et 2). Lorsqu'un U -résultant paramétrique (W, R) est calculé, on réduit R à des polynômes univariés paramétrés (par des spécialisations convenables des variables U_0, \dots, U_n) qui nous permettent par un calcul d'un p.g.c.d. paramétrique (voir le chapitre 2) de trouver le vecteur des multiplicités de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ d'une manière uniforme sur les valeurs $a \in W$ des paramètres (voir la section 3). La section 4 est consacrée à la description de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ par une représentation univariée polynomiale uniforme sur les valeurs des paramètres (voir théorème 3.5.3).

On s'intéresse dans ce chapitre aux systèmes surdéterminés, i.e. lorsque le nombre

d'équations est plus grand que celui des variables et on étudie le sous-ensemble \mathcal{U} de \mathcal{P} formé par les valeurs $a \in \mathcal{P}$ des paramètres tel que le système associé $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est de dimension zéro et n'admet pas de solutions à l'infini, i.e., la variété $V^{(a)}$ est un sous-ensemble fini de $P^n(\overline{F})$ et $V^{(a)} \cap V(X_0) = \emptyset$.

3.2 Résultant paramétrique

Définition 3.2.1 *Le système résultant d'un système polynomial $f_1 = \dots = f_k = 0$ est un ensemble fini de polynômes $R_1, \dots, R_s \in F[u_1, \dots, u_r]$ tel que pour toute valeur $a \in \mathcal{P}$ des paramètres, le système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ admet une solution dans $P^n(\overline{F})$ si et seulement si $R_1^{(a)} = 0, \dots, R_s^{(a)} = 0$.*

Proposition 3.2.2 *Chaque système $f_1 = \dots = f_k = 0$ admet un système résultant $R_1, \dots, R_s \in F[u_1, \dots, u_r]$.*

Preuve. Voir paragraphe 80 de [117], voir aussi [92, 37].□

Le nombre k d'équations du système paramétré $f_1 = \dots = f_k = 0$ est supposé $\geq n$. Dans cette section, nous étudions le cas $k = n + 1$ (i.e., $n + 1$ formes homogènes en $n + 1$ variables X_0, \dots, X_n). On peut montrer l'existence d'un seul polynôme $R \in F[u_1, \dots, u_r]$, appelé le résultant du système $f_1 = \dots = f_{n+1} = 0$ tel que pour tout $a \in \mathcal{P}$, le système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ admet une solution dans $P^n(\overline{F})$ si et seulement si $R^{(a)} = 0$ (voir [93, 117, 32, 35, 17, 18, 94]).

Proposition 3.2.3 *Soit R le résultant du système $f_1 = \dots = f_{n+1} = 0$. Alors*

$$\deg_{T_1, \dots, T_l}(R) \leq (n + 1)d_2d^n, \quad \deg_{u_1, \dots, u_r}(R) \leq (n + 1)\delta d^n$$

Preuve. Pour tout $1 \leq j \leq n + 1$, le degré de R par rapport aux coefficients de f_j est borné par

$$\frac{D_1 \cdots D_{n+1}}{D_j} \leq d^n$$

(Voir [93, 117, 32]). Ce qui prouve la proposition.□

Cette notion de résultant est une généralisation de celle du résultant de deux polynômes univariés qui est défini comme étant le déterminant du matrice de Sylvester. Dans le cas général, on peut exprimer le résultant R du système $f_1 = \dots = f_{n+1} = 0$ comme le quotient de deux déterminants :

$$R = \frac{\det(M)}{\det(M')}$$

M est une matrice carré d'ordre $N := \binom{n+\mathcal{D}}{n}$ où

$$\mathcal{D} := \sum_{1 \leq j \leq n+1} (D_j - 1) + 1 = \sum_{1 \leq j \leq n+1} D_j - n.$$

Les entrées de M sont parmi les coefficients de f_1, \dots, f_{n+1} dans $F[u_1, \dots, u_r]$, M' est une sous-matrice de M d'ordre

$$\binom{n + \mathcal{D}}{n} - \sum_{1 \leq j \leq n+1} \frac{D_1 \cdots D_{n+1}}{D_j}.$$

La matrice M est appelée la matrice de Macaulay [93] ou la matrice type de Sylvester associée au système $f_1 = \cdots = f_{n+1} = 0$, R est le résultant de Macaulay du système (voir [35, 32] pour la construction de ces matrices). Cette formalisation du résultant est valable seulement pour les valeurs $a \in \mathcal{P}$ des paramètres tel que $\det(M')$ ne s'annule pas en a . Pour éviter l'annulation de $\det(M')$ et pour calculer les résultants associés à tous les systèmes $f_1^{(a)} = \cdots = f_{n+1}^{(a)} = 0$ (pour tout $a \in \mathcal{P}$), Canny [18] (voir aussi [94]) introduit la notion du polynôme caractéristique généralisé du système $f_1 = \cdots = f_{n+1} = 0$ (une généralisation du polynôme caractéristique du matrice associée à un système linéaire homogène). On perturbe ce système par une nouvelle variable v en considérant les polynômes perturbés suivants :

$$\tilde{f}_j := f_j - vX_{j-1}^{D_j}, \quad 1 \leq j \leq n+1.$$

On peut montrer que le résultant \tilde{R} du système perturbé $\tilde{f}_1 = \cdots = \tilde{f}_{n+1} = 0$ s'écrit sous la forme :

$$\tilde{R} = \frac{\det(M - vI)}{\det(M' - vI)} \in F[u_1, \dots, u_r][v]$$

où I est la matrice unité convenable.

Définition 3.2.4 *Le polynôme \tilde{R} est appelé le polynôme caractéristique généralisé du système $f_1 = \cdots = f_{n+1} = 0$.*

Proposition 3.2.5 *Le polynôme \tilde{R} vérifie :*

$$a) \deg_v(\tilde{R}) = \sum_{1 \leq j \leq n+1} \frac{D_1 \cdots D_{n+1}}{D_j}.$$

b) *Le résultant R du système $f_1 = \cdots = f_{n+1} = 0$ est le terme constant de \tilde{R} dans $F[u_1, \dots, u_r]$.*

c) *La taille binaire de R est donnée par*

$$l(R) \leq M_1 M_2 r l d_2 (\delta d_1)^{O(1)} d^{O(n)}.$$

Preuve. Les points a) et b) sont évidents. Pour c), l'exercice 18, page 105 de [32] montre que R s'écrit sous la forme :

$$R = \frac{P}{Q}$$

où P (resp. Q) est le coefficient non nul dans $F[u_1, \dots, u_r]$ du monôme de degré minimal en v du numérateur (resp. dénominateur) de \tilde{R} . Les tailles de P et Q sont

$$l(P), l(Q) \leq \mathcal{D}^n(M_2 + 1) \leq \left((n+1)d\right)^n (M_2 + 1)$$

Leurs degrés par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $((n+1)d)^n \delta$ (resp. $((n+1)d)^n d_2$). La taille binaire de R s'obtient par application du lemme 1.3 de [22]. \square

Donc l'hypersurface de l'espace \mathcal{P} défini par le résultant R du système $f_1 = \dots = f_{n+1} = 0$ est le lieu de consistance du système. Pour décrire le sous-ensemble de \mathcal{P} là où le système n'admet pas de solutions à l'infini, on considère les polynômes homogènes suivants :

$$g_j := f_j(0, X_1, \dots, X_n) \in F[u_1, \dots, u_r, X_1, \dots, X_n], \quad 1 \leq j \leq n+1$$

Soit $R' \in F[u_1, \dots, u_r]$ le résultant du système $g_1 = \dots = g_{n+1} = 0$, alors nous avons la proposition suivante :

Proposition 3.2.6 *L'ouvert de \mathcal{P} défini par le polynôme $R' \in F[u_1, \dots, u_r]$ est l'ensemble des points $a \in \mathcal{P}$ tel que le système associé $f_1^{(a)} = \dots = f_{n+1}^{(a)} = 0$ n'admet pas de solutions à l'infini.*

Preuve. Pour tout $a \in \mathcal{P}$, le système $f_1^{(a)} = \dots = f_{n+1}^{(a)} = 0$ n'admet pas de solutions à l'infini si et seulement si le système $g_1^{(a)} = \dots = g_{n+1}^{(a)} = 0$ n'admet pas de solutions dans $P^{n-1}(\overline{F})$.

3.3 U-Résultant paramétrique

On suppose dans cette section que le nombre k d'équations du système paramétré $f_1 = \dots = f_k = 0$ est $\geq n$. La généralisation de la notion de résultant à des systèmes surdéterminés a été faite par Lazard [80, 81]. Dans cette section, nous étudions la notion de U -résultant du système $f_1 = \dots = f_k = 0$ qui était étudié par Kronecker et Van der Waerden [117] en introduisant une forme linéaire en X_0, \dots, X_n à coefficients indéterminés. Nous allons suivre dans cette section les constructions de [81] (voir aussi [58]).

Supposons que $d \geq D_1 \geq \dots \geq D_k$ et posons

$$\mathcal{D} = D_1 + \sum_{2 \leq i \leq n} (D_i - 1) \leq nd.$$

On introduit de nouvelles variables U_0, \dots, U_n qui sont algébriquement indépendantes sur $F(u_1, \dots, u_r, X_0, \dots, X_n)$ et une forme linéaire $f_{k+1} = U_0 X_0 + \dots + U_n X_n \in F(u_1, \dots, u_r, U_0, \dots, U_n)[X_0, \dots, X_n]$.

Notons par B_i (respectivement B) l'espace des polynômes homogènes en X_0, \dots, X_n à coefficients dans le corps $F(u_1, \dots, u_r, U_0, \dots, U_n)$ de degrés $\mathcal{D} - D_i$ (respectivement \mathcal{D}) pour tout $1 \leq i \leq k+1$ où $D_{k+1} = 1$.

On considère l'application $F(u_1, \dots, u_r, U_0, \dots, U_n)$ -linéaire suivante :

$$\Psi : B_1 \oplus \dots \oplus B_{k+1} \longrightarrow B$$

définie par :

$$\Psi(h_1, \dots, h_{k+1}) = \sum_{1 \leq i \leq k+1} h_i f_i \quad \text{pour tout } (h_1, \dots, h_{k+1}) \in B_1 \oplus \dots \oplus B_{k+1}.$$

Posons $N_i := \dim(B_i) = \binom{n+\mathcal{D}-D_i}{n}$, $1 \leq i \leq k+1$ et $N = \dim(B) = \binom{n+\mathcal{D}}{n}$ (les dimensions sont données en tant qu'espaces vectoriels sur $F(u_1, \dots, u_r, U_0, \dots, U_n)$).

Soit \mathcal{M} la matrice associée à Ψ dans les bases de B_1, \dots, B_{k+1}, B formées par les monômes. On peut représenter \mathcal{M} sous la forme :

$$\mathcal{M} = \mathcal{M}(u_1, \dots, u_r, U_0, \dots, U_n) = (\mathcal{M}_1 \quad \mathcal{M}_2)$$

où \mathcal{M}_1 est une matrice $N \times \left(\sum_{1 \leq i \leq k} N_i \right)$ à entrées dans $F[u_1, \dots, u_r]$ et \mathcal{M}_2 est une matrice $N \times N_{k+1}$ dont ses entrées sont des formes linéaires sur F en les variables U_0, \dots, U_n .

Remarque 3.3.1 Les entrées de \mathcal{M}_1 sont prises parmi les coefficients de f_1, \dots, f_k dans $F[u_1, \dots, u_r]$. La construction de \mathcal{M} dépend du rangement de polynômes f_1, \dots, f_k (sous la condition $D_1 \geq \dots \geq D_k$) et du classement des éléments des bases monomiales de B_1, \dots, B_{k+1}, B .

Exemple 3.3.2 Soit le système paramétré $(f_1, f_2, f_3) \subset \mathbb{Q}(t)[\sqrt{2}][u, v, X_0, X_1, X_2]$ suivant :

$$\begin{cases} f_1 = uvtX_0X_1 + \sqrt{2}vX_1^2 + X_0X_2 + X_2^2 \\ f_2 = uX_0^2 + vtX_1X_2 \\ f_3 = 3\sqrt{2}X_2^2 - 2tX_0X_1 + 5uX_1X_2 \end{cases}$$

On introduit la forme $f_4 = U_0X_0 + U_1X_1 + U_2X_2$, $D_1 = D_2 = D_3 = 2$ et $D_4 = 1$. Alors $\mathcal{D} = 3$, $N = 10$ et $N_i = 3$ ($1 \leq i \leq 3$), $N_4 = 6$. Donc \mathcal{M} est la matrice 10×15 suivante :

$$\mathcal{M} = \begin{pmatrix} 0 & 0 & 0 & u & 0 & 0 & 0 & 0 & 0 & U_0 & 0 & 0 & 0 & 0 & 0 \\ uvt & 0 & 0 & 0 & u & 0 & -2t & 0 & 0 & U_1 & U_0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & u & 0 & 0 & 0 & U_2 & 0 & U_0 & 0 & 0 & 0 \\ \sqrt{2}v & uvt & 0 & 0 & 0 & 0 & 0 & -2t & 0 & 0 & U_1 & 0 & U_0 & 0 & 0 \\ 0 & 1 & uvt & vt & 0 & 0 & 5u & 0 & -2t & 0 & U_2 & U_1 & 0 & U_0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 3\sqrt{2} & 0 & 0 & 0 & 0 & U_2 & 0 & 0 & U_0 \\ 0 & \sqrt{2}v & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & U_1 & 0 & 0 \\ 0 & 0 & \sqrt{2}v & 0 & vt & 0 & 0 & 5u & 0 & 0 & 0 & 0 & U_2 & U_1 & 0 \\ 0 & 1 & 0 & 0 & 0 & vt & 0 & 3\sqrt{2} & 5u & 0 & 0 & 0 & 0 & U_2 & U_1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3\sqrt{2} & 0 & 0 & 0 & 0 & 0 & U_2 \end{pmatrix}$$

Les lignes (resp. les colonnes) de \mathcal{M} sont indexées par les monômes en X_0, X_1, X_2 de degré $\mathcal{D} = 3$ (resp. $\mathcal{D} - D_i$ pour tout $1 \leq i \leq 4$). Ces monômes sont rangés en respectant l'ordre lexicographique avec $X_0 > X_1 > X_2$.

La description de l'ensemble \mathcal{U} et le calcul de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ pour tout $a \in \mathcal{U}$ sont basés sur le théorème suivant [80, 81] :

Théorème 3.3.3 1) Soit $a = (a_1, \dots, a_r) \in \mathcal{P}$, le système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ admet un nombre fini de solutions dans $P^n(\overline{F})$ si et seulement si $\text{rg}(\mathcal{M}^{(a)}) = N$ où $\mathcal{M}^{(a)} = \mathcal{M}(a_1, \dots, a_r, U_0, \dots, U_n)$ est à coefficients dans le corps $\overline{F}(U_0, \dots, U_n)$.

2) Pour tout $a \in \mathcal{U}$, l'idéal engendré par les déterminants de toutes les sous-matrices $N \times N$ de la matrice $\mathcal{M}^{(a)}$ est un idéal principal de $\overline{F}[U_0, \dots, U_n]$ engendré par leur plus grand commun diviseur $R_a \in \overline{F}[U_0, \dots, U_n]$ de degré égal à $N - \text{rg}(\mathcal{M}_1^{(a)})$.

3) Pour tout $a \in \mathcal{U}$, le polynôme homogène $R_a \in \overline{F}[U_0, \dots, U_n]$ se décompose sous la forme :

$$R_a = \prod_i L_i \quad \text{où} \quad L_i = \sum_{0 \leq j \leq n} \xi_j^{(i)} U_j \quad \text{avec} \quad \xi_j^{(i)} \in \overline{F}$$

chaque point $(\xi_0^{(i)} : \dots : \xi_n^{(i)}) \in P^n(\overline{F})$ est une solution du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$, sa multiplicité est égale à celle de L_i en tant que facteur de R_a , le nombre de solutions de ce système (comptées avec leurs multiplicités) est égale à $\deg_{U_0, \dots, U_n}(R_a)$.

Preuve. Voir [80, 81].□

Définition 3.3.4 Pour tout $a \in \mathcal{U}$, le polynôme homogène $R_a \in \overline{F}[U_0, \dots, U_n]$ est appelé le U -résultant du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$.

Pour tout $a \in \mathcal{U}$, le calcul du polynôme R_a est basé sur le lemme suivant [81] :

Lemme 3.3.5 Pour tout $a \in \mathcal{U}$, le polynôme R_a coïncide avec n'importe quel déterminant non nul d'une sous-matrice $N \times N$ de $\mathcal{M}^{(a)}$ qui contient $\text{rg}(\mathcal{M}_1^{(a)})$ colonnes de $\mathcal{M}_1^{(a)}$.

Le calcul des U -résultants paramétriques annoncés au début de ce chapitre se fait par l'algorithme suivant :

Lemme 3.3.6 Il existe un algorithme qui décompose \mathcal{U} en (au plus) N ensembles constructibles W_1, \dots, W_N . Pour chaque W_i , l'algorithme calcule un polynôme $R_i \in \overline{F}[u_1, \dots, u_r, U_0, \dots, U_n]$, appelé U -résultant paramétrique du système $f_1 = \dots = f_k = 0$. Chaque couple (W_i, R_i) vérifie :

a) R_i est homogène en U_0, \dots, U_n de degré $N - i \leq N$. En plus $\deg_u R_i \leq i\delta \leq N\delta$, $\deg_{T_1, \dots, T_l} R_i \leq i\delta_2 \leq N\delta_2$ et $l(R_i) \leq iM_2 \leq NM_2$.

b) Les degrés des équations et des inéquations qui définissent W_i par rapport à u et T_1, \dots, T_l sont respectivement bornés par $N\delta$ et $N\delta_2$. Leurs tailles binaires sont bornées par NM_2 .

c) Pour tout $a \in W_i$, $R_a = R_i^{(a)} \in \overline{F}[U_0, \dots, U_n]$ où R_a est le polynôme du point 3) du théorème 3.3.3 et $R_i^{(a)}$ est le polynôme obtenu à partir de R_i en spécialisant les paramètres par a , i.e., les coefficients des formes linéaires facteurs de $R_i^{(a)}$ sont les composantes des solutions à distance finie (solutions qui ne sont pas contenues dans l'hyperplan à l'infini $\{X_0 = 0\} \subset P^n(\overline{F})$) du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$. En particulier, le nombre de solutions (comptées avec leurs multiplicités) est constant sur W_i et il est égal à $\deg_{U_0, \dots, U_n}(R_i)$.

Cet algorithme se fait avec

$$(N\delta d_1 d_2)^{O(rl)}$$

opérations élémentaires dans H . Sa complexité binaire est

$$M_1 M_2 (N\delta d_1 d_2)^{O(rl)}.$$

Preuve. Considérons la matrice de Macaulay \mathcal{M} de taille $N \times \left(\sum_{1 \leq i \leq k+1} N_i\right)$ à entrées dans $F'[u_1, \dots, u_r]$ où $F' := H(T_1, \dots, T_l, U_0, \dots, U_n)[\eta]$. Appliquons l'algorithme de Gauss paramétrique du chapitre 2 sur \mathcal{M} . Cet algorithme décrit un ensemble constructible W où le rang de \mathcal{M} est maximal, i.e., pour tout $a \in W$, $rg(\mathcal{M}^{(a)}) = N$. Donc par le point 1) du théorème 3.3.3, W est le sous-ensemble de \mathcal{P} où le système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ admet un nombre fini de solutions dans $P^n(\overline{F})$. Cet algorithme permet aussi de décomposer \mathcal{P} en N ensembles constructibles \mathcal{U}_i deux à deux disjoints qui vérifient :

- Le rang de \mathcal{M}_1 est constant sur chaque \mathcal{U}_i et il est égal à i , i.e., pour tout $a \in \mathcal{U}_i$, $rg(\mathcal{M}_1^{(a)}) = i$.

- Les degrés des équations et des inéquations qui définissent \mathcal{U}_i par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $N\delta$ (resp. Nd_2). Leurs tailles binaires sont bornées par

$$NM_2.$$

Pour chaque \mathcal{U}_i , calculons $R_i \in F[u_1, \dots, u_r, U_0, \dots, U_n]$ le déterminant d'une sous-matrice $N \times N$ de \mathcal{M} qui contient i colonnes de \mathcal{M}_1 .

Soient $\Delta_i = \deg_{U_0, \dots, U_n} R_i = N - i$ et $I_i \in F[u_1, \dots, u_r]$ le coefficient de $U_0^{\Delta_i}$ dans R_i . Posons

$$W_i = \mathcal{U}_i \cap W \cap \{I_i \neq 0\}$$

Les ensembles W_1, \dots, W_N forment une partition de \mathcal{U} et les couples (W_i, R_i) ($1 \leq i \leq N$) vérifient les points a) et b) du lemme. Le point c) est assuré par le lemme 3.3.5 et l'existence de I_i . L'estimation de la complexité de cet algorithme se déduit de celle de l'algorithme de Gauss paramétrique. \square

Remarque 3.3.7 Si $k = n$, on obtient un seul couple (\mathcal{U}, R) qui vérifie les points a), b) et c) du lemme 3.3.6 où

$$\mathcal{U} = W \cap \{I \neq 0\}$$

W est le sous-ensemble constructible de \mathcal{P} calculé dans la preuve du lemme 3.3.6. Le U -résultant paramétrique R du système f_1, \dots, f_n est le résultant du système $f_1, \dots, f_n, f_{n+1} = U_0 X_0 + \dots + U_n X_n$ ($n+1$ équations homogènes en $n+1$ variables) au sens du section précédente, i.e.,

$$R = \frac{\det(\mathcal{M})}{\det(\mathcal{M}')}$$

où \mathcal{M}' est une sous-matrice de \mathcal{M}_1 ($\det(\mathcal{M}')$ est indépendante des variables U_0, \dots, U_n). Par une perturbation du système f_1, \dots, f_n, f_{n+1} , on peut calculer R par le point b) de la proposition 3.2.5.

3.4 Vecteur constant des multiplicités

On fixe un certain couple (W_i, R_i) du lemme 3.3.6 ($1 \leq i \leq N$). Pour tout $a \in W_i$, le polynôme homogène $R_i^{(a)}$ se décompose sous la forme

$$R_i^{(a)} = L_1^{s_1} \dots L_h^{s_h}$$

où les L_j ($1 \leq j \leq h$) sont de formes linéaires distinctes en U_0, \dots, U_n à coefficients dans \overline{F} . Les solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ sont données par les coefficients de L_1, \dots, L_h au sens du point 3) du théorème 3.3.3. Le vecteur $s = (s_1, \dots, s_h) \in \mathbb{N}^h$ est appelé le vecteur des multiplicités de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ (pas d'ordre sur la séquence s_1, \dots, s_h). On voudrait dans cette section calculer uniformément les vecteurs des multiplicités pour tout $a \in W_i$ i.e., décomposer W_i en un nombre fini d'ensembles constructibles tel que le vecteur des multiplicités est constant sur chacun d'eux.

Pour tout $1 \leq j \leq n$, considérons les polynômes paramétrés suivants :

$$Q_j := R_i(U_0, 0, \dots, 0, U_j, 0, \dots, 0) \in F[u_1, \dots, u_r, U_0, U_j]$$

et

$$G_j(Z^{p^{\nu_j}}) = Q_j(Z, -1) \in F[u_1, \dots, u_r][Z] \quad (3.1)$$

où Z est une nouvelle variable et p^{ν_j} est une puissance maximale qu'on peut extraire, i.e, $G_j \notin F[u_1, \dots, u_r][Z^p]$ ($p^{\nu_j} = 1$ si $\text{car}(F) = 0$). Le lemme suivant détermine la relation entre les solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ et les racines dans \overline{F} des polynômes $G_1^{(a)}, \dots, G_n^{(a)} \in \overline{F}[Z]$ (pour tout $a \in W_i$).

Lemme 3.4.1 Soient $a \in W_i$ et $\xi = (\xi_0 : \dots : \xi_n) \in P^n(\overline{F})$. Si ξ est une solution du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ de multiplicité β alors pour tout $1 \leq j \leq n$,

$$\left(\frac{\xi_j}{\xi_0} \right)^{p^{\nu_j}} \text{ est une racine de } G_j^{(a)} \in \overline{F}[Z] \text{ de multiplicité } \geq \beta.$$

Preuve. Si ξ est une solution du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ de multiplicité β alors $(\xi_0 U_0 + \dots + \xi_n U_n)^\beta$ divise $R_i^{(a)}$. Donc pour tout $1 \leq j \leq n$, $(\xi_0 U_0 + \xi_j U_j)^\beta$ divise $Q_j^{(a)}(U_0, U_j)$, ce qui prouve le lemme. \square

Pour calculer les vecteurs constants des multiplicités des systèmes $f_1^{(a)} = \dots = f_k^{(a)} = 0$ ($a \in W_i$), nous aurons besoin d'un algorithme qui calcule un vecteur constant des multiplicités des racines d'un polynôme univarié paramétré :

Lemme 3.4.2 *Soit $G \in F[u_1, \dots, u_r][Z]$ un polynôme univarié paramétré de degré par rapport à Z (resp. u_1, \dots, u_r et T_1, \dots, T_l) borné par d' (resp. δ' et d'_2), de taille binaire M'_2 . Il existe un algorithme qui décompose l'espace des paramètres \mathcal{P} en*

$$(\delta' + d')^{O(r)}$$

ensembles constructibles \mathcal{V} deux à deux disjoints qui vérifient :

a) *Les degrés des équations et des inéquations qui définissent \mathcal{V} par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $(\delta' + d')^{O(1)}$ (resp. $d'_2(d_1(\delta' + d'))^{O(1)}$). Les tailles binaires de leurs coefficients dans H sont bornées par*

$$\left(M_1 + M'_2 + (l + r) \log_2(d'_2) \right) \left(d_1(\delta' + d') \right)^{O(1)}$$

b) *Pour chaque \mathcal{V} , l'algorithme calcule un vecteur $s = (s_1, \dots, s_h) \in \mathbb{N}^h$ tel que pour tout $a \in \mathcal{V}$, le vecteur s est le vecteur des multiplicités des racines du polynôme $G^{(a)} \in \overline{F}[Z]$.*

c) *Cet algorithme se fait avec*

$$(d_1 d'_2)^{O(l)} (\delta' + d')^{O(r+l)}$$

opérations dans H . Sa complexité binaire est

$$(M_1 M'_2)^{O(1)} (d_1 d'_2)^{O(l)} (\delta' + d')^{O(r+l)}.$$

Preuve. Pour tout $1 \leq j \leq \deg_Z(G) \leq d'$, l'algorithme A2 du chapitre 2 permet de calculer un plus grand commun diviseur paramétrique de la famille $\{G, G', \dots, G^{(j)}\} \subset F[u_1, \dots, u_r][Z]$ des dérivées successives de G . Cet algorithme représente ce p.g.c.d. sous la forme :

$$A_{j,m} Z^m + A_{j,m-1} Z^{m-1} + \dots + A_{j,0} \in F[u_1, \dots, u_r][Z]$$

avec $\deg_{u_1, \dots, u_r}(A_{j,\alpha}) \leq (\delta' + d')^{O(1)}$ pour tout $0 \leq \alpha \leq m \leq d' - j$. Le degré de p.g.c.d. $(G, G', \dots, G^{(j)})$ pour tout $1 \leq j \leq d'$ détermine le vecteur des multiplicités des racines de G . Considérons les ensembles constructibles suivants :

$$\mathcal{V}_{j,\alpha} := \{A_{j,\alpha} *_{j,\alpha} 0\} \subset \mathcal{P}$$

où $*_{j,\alpha} \in \{=, \neq\}$. Ces ensembles constituent une décomposition de \mathcal{P} , sur chacun d'eux le vecteur des multiplicités des racines de G est constant. Les degrés, les tailles binaires ainsi que la borne de complexité se déduisent de ceux de l'algorithme A2 du chapitre 2. \square

Nous pouvons maintenant énoncer le résultat principal de cette section, i.e., le calcul des vecteurs constants des multiplicités de solutions des systèmes $f_1^{(a)} = \dots = f_k^{(a)} = 0$ ($a \in W_i$) :

Lemme 3.4.3 *Soit $(W_i, R_i), 1 \leq i \leq N$ un couple donné au lemme 3.3.6 (R_i est un U -résultant paramétrique du système $f_1 = \dots = f_k = 0$). Il existe un algorithme qui décompose W_i en*

$$(N\delta)^{O(nr)}$$

ensembles constructibles \mathcal{W} deux à deux disjoints qui vérifient :

a) Les degrés des équations et des inéquations qui définissent \mathcal{W} par rapport à u_1, \dots, u_r (resp. T_1, \dots, T_l) sont bornés par $(N\delta)^{O(1)}$ (resp. $d_2(N\delta d_1)^{O(1)}$). Les tailles binaires de leurs coefficients dans H sont bornées par

$$\left(M_1 + M_2 + rl \log_2(d_2)\right) \left(N\delta d_1\right)^{O(1)}$$

b) Pour chaque \mathcal{W} , l'algorithme calcule un vecteur $s = (s_1, \dots, s_h) \in \mathbb{N}^h$ tel que pour tout $a \in \mathcal{W}$, le vecteur s est le vecteur des multiplicités de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$

c) Cet algorithme se fait avec

$$(d_1 d_2)^{O(l)} (N\delta)^{O(r+l)}$$

opérations dans H . Sa complexité binaire est

$$(M_1 M_2)^{O(1)} (d_1 d_2)^{O(l)} (N\delta)^{O(r+l)}$$

Preuve. Considérons les polynômes paramétrés $G_1, \dots, G_n \in F[u_1, \dots, u_r][Z]$ définis ci-dessus par (3.1). L'application de l'algorithme du lemme 3.4.2 sur G_1 permet de décomposer W_i en un nombre fini d'ensembles constructibles W_{i,q_1} chacun avec un vecteur constant $s^{(1)} = (s_1^{(1)}, \dots, s_{h_1}^{(1)}) \in \mathbb{N}^{h_1}$ des multiplicités des racines de G_1 . De nouveau, W_{i,q_1} se décompose en des ensembles constructibles W_{i,q_1,q_2} chacun avec un vecteur constant $s^{(2)} = (s_1^{(2)}, \dots, s_{h_2}^{(2)}) \in \mathbb{N}^{h_2}$ des multiplicités des racines de G_2 et ainsi de suite. On obtient à la fin une partition de W_i en un nombre fini d'ensembles constructibles $W_{i,q_1,\dots,q_n}^{(n)}$. Pour chaque ensemble \mathcal{W} parmi eux, on pose $h = \min(h_1, \dots, h_n)$ et pour tout $1 \leq j \leq h$,

$$s_j := \min(s_j^{(1)}, \dots, s_j^{(n)})$$

Alors par le lemme 3.4.1, $s := (s_1, \dots, s_h)$ est un vecteur constant des multiplicités de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ pour tout $a \in \mathcal{W}$. Les degrés, les tailles binaires

ainsi que la borne de complexité se déduisent du lemme 3.4.2 en tenant compte que pour tout $1 \leq j \leq n$,

$$\deg_Z(G_j) \leq \deg_{U_0, \dots, U_n}(R_i) \leq N, \quad \deg_{u_1, \dots, u_r}(G_j) \leq N\delta, \quad \deg_{T_1, \dots, T_l}(G_j) \leq Nd_2$$

et la taille binaire de G_j est bornée par NM_2 . \square

3.5 Shape lemma paramétrique

Fixons un ensemble constructible $\mathcal{W} \subset W_i$ du lemme 3.4.3 avec le U -résultant paramétrique R_i du système $f_1 = \dots = f_k = 0$ et les polynômes univariés paramétrés $G_1, \dots, G_n \in F[u_1, \dots, u_r][Z]$ définis par (3.1). Nous avons vu que pour tout $a \in \mathcal{W}$ les composantes des solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ sont les racines des polynômes univariés $G_1^{(a)}, \dots, G_n^{(a)} \in \overline{F}[Z]$ (lemme 3.4.1). Dans cette section nous allons partager de nouveau \mathcal{W} en un nombre fini d'ensembles constructibles et exprimer les solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ comme des fonctions polynomiales des racines d'un polynôme univarié à coefficients dans \overline{F} d'une manière uniforme sur chaque ensemble constructible (voir théorème 3.5.3).

Soient $K = F(u_1, \dots, u_r)$ le corps de fonctions rationnelles en les paramètres et pour tout $1 \leq j \leq n$, λ_j une racine de $Q_j(Z, -1)$ dans \overline{K} . Chaque $\lambda_j^{p^{\nu_j}}$ est algébrique séparable sur K de polynôme minimal diviseur de G_j dans $K[Z]$. Le lemme suivant construit un élément primitif θ de l'extension $E := K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_n^{p^{\nu_n}}]$ sur K avec son polynôme minimal $\chi \in K[Z]$.

Lemme 3.5.1 *Sous les notations et les hypothèses ci-dessus, il existe un algorithme qui calcule un élément primitif θ de l'extension $E := K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_n^{p^{\nu_n}}]$ sur K avec son polynôme minimal $\chi \in K[Z]$ vérifiant :*

- $\deg_{u_1, \dots, u_r}(\chi) \leq \delta(Nd_1)^{O(n)}, \deg_{T_1, \dots, T_l}(\chi) \leq d_2(Nd_1)^{O(n)}$. La taille binaire de χ est bornée par $(M_1 + M_2)rld_2(Nd_1)^{O(n)}$.

- Cet algorithme se fait avec

$$(\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$$

opérations dans H . Sa complexité binaire est

$$(pM_1M_2)^{O(1)}(\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$$

Preuve. Nous construisons un élément primitif θ_j de l'extension finie et séparable $E_j := K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_j^{p^{\nu_j}}]$ sur K avec son polynôme minimal χ_j par induction sur j .

Pour $j = 1$, calculons $\chi_1 \in K[Z]$ un facteur irréductible unitaire de G_1 dans $K[Z]$

admettant $\lambda_1^{p^{\nu_1}}$ comme racine par application de l'algorithme de factorisation de polynômes multivariés de [22] (voir aussi [58]) sur le corps $H(T_1, \dots, T_l, u_1, \dots, u_r)[\eta]$, i.e, χ_1 est le polynôme minimal de $\lambda_1^{p^{\nu_1}}$ sur K . Le lemme 1.3 de [22] montre que les degrés de χ_1 par rapport à u_1, \dots, u_r et T_1, \dots, T_l sont respectivement bornés par $\delta(Nd_1)^{O(1)}$ et $d_2(Nd_1)^{O(1)}$. Sa taille binaire est

$$l(\chi_1) \leq (M_1 + M_2)rd_2(Nd_1)^{O(1)}.$$

La factorisation de G_1 [22] se fait avec

$$(\delta Nd_1 d_2)^{O(rl)}$$

opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} (\delta Nd_1 d_2)^{O(rl)}.$$

Supposons qu'à l'étape $j - 1$, un élément primitif θ_{j-1} de l'extension $E_{j-1} = K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_{j-1}^{p^{\nu_{j-1}}}]$ sur K est calculé avec son polynôme minimal $\chi_{j-1} \in K[Z]$ vérifiant $\deg_u(\chi_{j-1}) \leq \delta(Nd_1)^{O(j)}$, $\deg_{T_1, \dots, T_l}(\chi_{j-1}) \leq d_2(Nd_1)^{O(j)}$ et $l(\chi_{j-1}) \leq M_1 M_2 rd_2(Nd_1)^{O(j)}$.

Calculons $h_j \in E_{j-1}[Z]$ un facteur irréductible unitaire de G_j admettant $\lambda_j^{p^{\nu_j}}$ comme racine, i.e, h_j est le polynôme minimal de $\lambda_j^{p^{\nu_j}}$ sur E_{j-1} [22]. De même $\deg_u(h_j) \leq \delta(Nd_1)^{O(1)}$, $\deg_{T_1, \dots, T_l}(h_j) \leq d_2(Nd_1)^{O(1)}$ et $l(h_j) \leq M_1 M_2 rd_2(Nd_1)^{O(1)}$ (lemme 1.3 de [22]). La complexité de factorisation de G_j sur E_{j-1} est égale à celle de G_1 ci-dessus. Nous avons l'extension

$$E_j = K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_j^{p^{\nu_j}}] = E_{j-1}[\lambda_j^{p^{\nu_j}}] = K[\theta_{j-1}, \lambda_j^{p^{\nu_j}}]$$

finie et séparable sur K de degré inférieur ou égale à N . Fixons des éléments $0 = c_1, \dots, c_N \in H$ distincts deux à deux et considérons les éléments $\theta_{j-1} + c_1 \lambda_j^{p^{\nu_j}}, \dots, \theta_{j-1} + c_N \lambda_j^{p^{\nu_j}}$ de E_j . Le théorème de l'élément primitif implique l'existence d'un élément $\theta_j = \theta_{j-1} + c \lambda_j^{p^{\nu_j}}$ parmi eux qui est un élément primitif de l'extension E_j sur K .

Pour calculer le polynôme minimal χ_j de θ_j sur K , il suffit d'exprimer les puissances de θ_j dans la base $\theta_{j-1}^\alpha \left(\lambda_j^{p^{\nu_j}} \right)^\beta$, $0 \leq \alpha < \deg_Z(\chi_{j-1})$, $0 \leq \beta < \deg_Z(h_j)$ de E_j sur K . Les coefficients de χ_j forment une solution non triviale d'un certain système linéaire homogène à coefficients dans K (si ce système n'admet pas de solutions non triviales alors l'algorithme considère un autre élément c parmi c_1, \dots, c_N). C'est un système carré d'ordre $\left(\deg_Z(\chi_{j-1}) \right) \left(\deg_Z(h_j) \right) = \deg_Z(\chi_j) \leq N$, les degrés de ses entrées par rapport à u_1, \dots, u_r et T_1, \dots, T_l sont respectivement bornés par $\delta(Nd_1)^{O(j)}$ et $d_2(Nd_1)^{O(j)}$, leurs tailles binaires sont bornées par $M_1 M_2 rd_2(Nd_1)^{O(j)}$. Donc par les formules de Cramer, les degrés des coefficients de χ_j par rapport à u_1, \dots, u_r et T_1, \dots, T_l sont respectivement bornés par $\delta(Nd_1)^{O(j)}$ et $d_2(Nd_1)^{O(j)}$, leurs tailles binaires sont bornées

par $(M_1 + M_2)rld_2(Nd_1)^{O(j)}$. La résolution de ces systèmes (pour tous les $c \in \{c_1, \dots, c_N\}$) se fait avec

$$(\delta d_2)^{O(rl)}(Nd_1)^{O(jrl)}$$

opérations dans H . Sa complexité binaire est

$$M_1 M_2 (\delta d_2)^{O(rl)}(Nd_1)^{O(jrl)}.$$

Prenons $\theta := \theta_n$ et $\chi := \chi_n \in K[Z]$ alors $E_n = K[\lambda_1^{p^{\nu_1}}, \dots, \lambda_n^{p^{\nu_n}}] = K[\theta] = E$. \square

Lemme 3.5.2 *On peut calculer de polynômes $\psi_1, \dots, \psi_n \in K[Z]$ de degrés strictement inférieurs à N tels que pour tout $1 \leq j \leq n$,*

$$\lambda_j^{p^{\nu_j}} = \psi_j(\theta)$$

Ces polynômes vérifient :

- *Les degrés des coefficients de ψ_1, \dots, ψ_n par rapport à u_1, \dots, u_r et T_1, \dots, T_l sont respectivement bornés par $\delta(Nd_1)^{O(n)}$ et $d_2(Nd_1)^{O(n)}$. Leurs tailles binaires sont bornées par $(M_1 + M_2)rld_2(Nd_1)^{O(n)}$.*

- *Le calcul de ψ_1, \dots, ψ_n se fait avec*

$$(\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$$

opérations dans H . Sa complexité binaire est

$$M_1 M_2 (\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$$

Preuve. Le calcul de ψ_1, \dots, ψ_n se fait par récurrence sur j . Pour $j = 1$, on a $\lambda_1^{p^{\nu_1}} = \theta_1$. Supposons que $\lambda_1^{p^{\nu_1}}, \dots, \lambda_{j-1}^{p^{\nu_{j-1}}}$ sont exprimés en fonction de θ_{j-1} par de polynômes à coefficients dans K de degrés par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l respectivement bornés par $\delta(Nd_1)^{O(j)}$ et $d_2(Nd_1)^{O(j)}$. Puisque $\theta_j = \theta_{j-1} + c\lambda_j^{p^{\nu_j}}$ (voir preuve du lemme 3.5.1), on exprime les puissances de θ_j dans la base $\theta_{j-1}^\alpha \left(\lambda_j^{p^{\nu_j}}\right)^\beta$, $0 \leq \alpha < \deg_Z(\chi_{j-1})$, $0 \leq \beta < \deg_Z(h_j)$ de E_j sur K . Pour exprimer θ_{j-1} et $\lambda_j^{p^{\nu_j}}$ comme de combinaisons linéaires des puissances de θ_j à coefficients dans K , il suffit de résoudre un système linéaire carré d'ordre $\leq N$. Par les formules de Cramer, les degrés de l'expression de $\lambda_j^{p^{\nu_j}}$ par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l sont respectivement bornés par $\delta(Nd_1)^{O(j)}$ et $d_2(Nd_1)^{O(n)}$, sa taille binaire est bornée par $M_1 M_2 rld_2(Nd_1)^{O(j)}$. Par substitution de l'expression de θ_{j-1} dans les expressions de $\lambda_1^{p^{\nu_1}}, \dots, \lambda_{j-1}^{p^{\nu_{j-1}}}$, on obtient les expressions de $\lambda_1^{p^{\nu_1}}, \dots, \lambda_{j-1}^{p^{\nu_{j-1}}}$ comme des combinaisons linéaires des puissances de θ_j à coefficients dans K . Cette résolution se fait avec

$$(\delta d_2)^{O(rl)}(Nd_1)^{O(jrl)}$$

opérations dans H . Sa complexité binaire est

$$M_1 M_2 (\delta d_2)^{O(rl)} (N d_1)^{O(jrl)}. \square$$

Désignons par $\psi \in F[u_1, \dots, u_r]$ le P.P.C.M des dénominateurs des coefficients de $\chi, \psi_1, \dots, \psi_n$. Considérons l'ensemble constructible $P_1 = \mathcal{W} \cap \{\psi = 0\} \subset \mathcal{P}$.

Pour tout $a \in \mathcal{W} \setminus P_1$, une représentation paramétrique de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est donnée par (voir les lemmes 3.4.1 et 3.5.2) :

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} = \psi_1^{(a)}(\theta) \\ \vdots \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_1}} = \psi_n^{(a)}(\theta) \end{cases}$$

Cette représentation de solutions du système $f_1 = \dots = f_k = 0$ est valable seulement sur $\mathcal{W} \setminus P_1$. Le théorème suivant montre qu'on peut construire des représentations paramétriques pour toutes les valeurs des paramètres $a \in \mathcal{W} \cap P_1$. Ce théorème résume l'algorithme principal de ce chapitre :

Théorème 3.5.3 *Soient $f_1 = \dots = f_k = 0$ un système paramétré et \mathcal{U} un sous-ensemble de \mathcal{P} vérifiant les conditions ci-dessus. Il existe un algorithme qui partage \mathcal{U} en*

$$(N \delta d_1)^{O(nr^2)} \leq (\delta d d_1)^{O(n^2 r^2)}$$

ensembles constructibles \mathcal{A} deux à deux disjoints qui vérifient :

1) *Les degrés des équations et des inéquations qui définissent \mathcal{A} par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l sont bornés par*

$$d_2 \delta^{O(r)} (N d_1)^{O(nr)} \leq d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$$

Leurs tailles binaires sont bornées par

$$(M_1 + M_2) l d_2 \delta^{O(r)} (N d_1)^{O(nr)} \leq (M_1 + M_2) l d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$$

2) *Le nombre D des solutions est constant sur \mathcal{A} , ce nombre est borné par $N \leq (nd)^n$.*

3) *Le vecteur des multiplicités est constant sur \mathcal{A} , ce vecteur est calculé par l'algorithme.*

4) *Pour chaque \mathcal{A} , l'algorithme calcule des polynômes $\chi, \psi_1, \dots, \psi_n \in F(u_1, \dots, u_r)[Z]$ de degrés inférieurs ou égaux à D . Toute spécialisation des paramètres $a \in \mathcal{A}$ vérifie :*

- Aucun des dénominateurs des coefficients de $\chi, \psi_1, \dots, \psi_n$ ne s'annule en a .
- Les degrés des coefficients de $\chi, \psi_1, \dots, \psi_n$ par rapport à u_1, \dots, u_r et par rapport à T_1, \dots, T_l sont bornés par

$$d_2 \delta^{O(r)} (Nd_1)^{O(nr)} \leq d_2 \delta^{O(r)} (dd_1)^{O(n^2r)}$$

Leurs tailles binaires sont bornées par

$$(M_1 + M_2) l d_2 \delta^{O(r)} (Nd_1)^{O(nr)} \leq (M_1 + M_2) l d_2 \delta^{O(r)} (dd_1)^{O(n^2r)}$$

- Une représentation paramétrique des solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est donnée par

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} = \psi_1^{(a)}(\theta) \\ \vdots \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_n}} = \psi_n^{(a)}(\theta) \end{cases}$$

En plus, $\theta = \sum_{1 \leq j \leq n} \gamma_j \left(\frac{X_j}{X_0}\right)^{p^{\nu_j}}$ avec $0 \leq \gamma_j \leq D \leq N$ est un entier.

5) Cet algorithme se fait avec

$$(\delta d_2)^{O(r^2l)} (Nd_1)^{O(nr^2l)} \leq (\delta d_2)^{O(r^2l)} (dd_1)^{O(n^2r^2l)}$$

opérations dans H . Sa complexité binaire est

$$(pM_1M_2)^{O(1)} (\delta d_2)^{O(r^2l)} (Nd_1)^{O(nr^2l)} \leq (pM_1M_2)^{O(1)} (\delta d_2)^{O(r^2l)} (dd_1)^{O(n^2r^2l)}$$

Preuve. La preuve se fait par une continuation de la discussion juste avant ce théorème. Reprenons la variété $\mathcal{W} \cap P_1 \subset \overline{F}^r$, l'algorithme de résolution de systèmes algébriques de [23, 58, 22] (voir aussi le chapitre 2) calcule pour chaque composante irréductible S_1 de codimension m de la variété $\mathcal{W} \cap P_1$ un point générique *efficace* défini par l'isomorphisme suivant :

$$F(t_1, \dots, t_{r-m})[\mu] \cong F(S_1) \quad (3.2)$$

où t_1, \dots, t_{r-m} sont algébriquement indépendantes sur F , μ est algébrique séparable sur le corps $F(t_1, \dots, t_{r-m})$ de polynôme minimal $\Phi \in F(t_1, \dots, t_{r-m})[Z]$. Cet isomorphisme permet d'exprimer chaque variable u_i ($1 \leq i \leq r$) comme élément de $F(t_1, \dots, t_{r-m})[\mu]$.

Par substitution de ces expressions dans les polynômes $G_j \in F[u_1, \dots, u_r][Z]$, on obtient de polynômes $g_j \in F(t_1, \dots, t_{r-m})[\mu][Z]$ avec $\deg_Z(g_j) \leq N$.

L'application de cet algorithme [23, 58, 22] se fait avec

$$(d_1 \Delta^r \Delta_2)^{O(rl)}$$

opérations dans H où $\Delta = \delta^{O(1)}(Nd_1)^{O(n)}$ est une borne supérieure de degrés des équations de $\mathcal{W} \cap P_1$ par rapport à u_1, \dots, u_r , $\Delta_2 = d_2 \delta^{O(1)}(Nd_1)^{O(n)}$ est une borne supérieure de degrés des équations de $\mathcal{W} \cap P_1$ par rapport à T_1, \dots, T_l (voir lemme 3.3.6, lemme 3.4.3 et lemme 3.5.2 ci-dessus). Ce nombre est borné par

$$(\delta d_2)^{O(r^2 l)} (Nd_1)^{O(nr^2 l)}$$

Sa complexité binaire est bornée par

$$(pM_1 M'_2)^{O(1)} (d_1 \Delta^r \Delta_2)^{O(r l)}$$

où $M'_2 = (M_1 + M_2) r l d_2 \delta^{O(1)} (Nd_1)^{O(n)}$ est taille binaire des coefficients des équations de $\mathcal{W} \cap P_1$ dans H . Cette complexité est bornée par

$$(pM_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (Nd_1)^{O(nr^2 l)}$$

La même procédure précédente (voir lemme 3.5.1) calcule un élément primitif $\theta^{(1)}$ de l'extension $K'[\lambda_1^{p^{\nu_1}}, \dots, \lambda_n^{p^{\nu_n}}]$ sur K' avec son polynôme minimal $\chi \in K'[Z]$ où $K' := F(t_1, \dots, t_{r-m})[\theta]$ et $\lambda_j^{p^{\nu_j}}$ est une racine de $g_j \in K'[Z]$ dans $\overline{K'}$.

En tenant compte des degrés des expressions des variables u_1, \dots, u_r comme élément de $F(t_1, \dots, t_{r-m})[\mu]$ donnés par l'algorithme de Chistov-Grigoriev (voir chapitre 2), les degrés de chaque g_j par rapport à μ, t_1, \dots, t_{r-m} et par rapport à T_1, \dots, T_l sont bornés par

$$d_2 \delta^{O(r)} (Nd_1)^{O(nr)}$$

Sa taille binaire est

$$(M_1 + M_2) l d_2 \delta^{O(r)} (Nd_1)^{O(nr)}$$

Ils existent de polynômes $\psi_1, \dots, \psi_n \in K'[Z]$ de degrés inférieurs ou égale à N tels que pour tout $1 \leq j \leq n$,

$$\lambda_j^{p^{\nu_j}} = \psi_j(\theta^{(1)}).$$

Désignons par $\psi^{(1)} \in F[t_1, \dots, t_{r-m}]$ le P.P.C.M des dénominateurs des coefficients de $\chi, \psi_1, \dots, \psi_n$. Exprimons $\psi^{(1)}$ (resp. $\chi, \psi_1, \dots, \psi_n$) comme un élément de $F[u_1, \dots, u_r]$ (resp. des éléments de $F(u_1, \dots, u_r)[Z]$) en utilisant l'isomorphisme (3.2). Considérons la variété $P_2 = S_1 \cap \{\psi^{(1)} = 0\} \subset \overline{F}^r$.

Pour tout $a \in S_1 \setminus P_2$, une représentation paramétrique de solutions du système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ est donnée par (voir les lemmes 3.4.1 et 3.5.2) :

$$\chi^{(a)}(\theta^{(1)}) = 0, \quad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} &= \psi_1^{(a)}(\theta^{(1)}) \\ \vdots & \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_1}} &= \psi_n^{(a)}(\theta^{(1)}) \end{cases}$$

Les lemmes 3.5.1 et 3.5.2 ainsi que l'isomorphisme (3.2) montrent que les degrés de $\chi, \psi_1, \dots, \psi_n$ par rapport à u_1, \dots, u_r et par rapport T_1, \dots, T_l sont bornés par $d_2 \delta^{O(r)} (Nd_1)^{O(nr)}$. Leurs tailles binaires sont bornées par $(M_1 + M_2) l d_2 \delta^{O(r)} (Nd_1)^{O(nr)}$. La complexité de ce calcul est

$$(\delta d_2)^{O(rl)} (Nd_1)^{O(nrl)}$$

On applique de nouveau la même procédure sur la variété P_2 , l'algorithme se termine après un nombre fini d'étapes (au plus r étapes) car à chaque étape la dimension de la variété diminue ($\dim(P_2) = \dim(S_1) - 1 = r - m - 1$).

Les bornes sur les degrés et sur la complexité totale de cet algorithme se déduisent de la discussion ci-dessus et des lemmes 3.3.6, 3.4.3, 3.5.1 et 3.5.2. Il reste à estimer le nombre des ensembles constructibles \mathcal{A} . En effet, le nombre des W_i est au plus N (lemme 3.3.6) et le nombre des \mathcal{W} est $\leq (N\delta)^{O(nr)}$ (lemme 3.4.3). Les degrés des équations qui définissent $\mathcal{W} \cap P_1$ par rapport à u_1, \dots, u_r sont bornés par $(N\delta d_1)^{O(n)}$ (voir les lemmes 3.3.6, 3.4.3 et 3.5.2). Le nombre des composantes S_1 de $\mathcal{W} \cap P_1$ (de même pour le nombre des composantes de chaque $S_1 \cap P_2$) est borné par

$$\deg(\mathcal{W} \cap P_1) \leq (N\delta d_1)^{O(nr)}$$

Puisque le nombre d'étapes est au plus r alors le nombre total \mathcal{N} des ensembles \mathcal{A} du théorème est :

$$\begin{aligned} \mathcal{N} &\leq N(N\delta)^{O(nr)} (N\delta d_1)^{O(nr^2)} \\ &\leq (N\delta d_1)^{O(nr^2)}. \square \end{aligned}$$

Chapitre 4

Factorisation absolue des polynômes paramétrés

4.1 Introduction et notations

Considérons un polynôme paramétré $f \in F[u_1, \dots, u_r][Z_0, \dots, Z_n]$ vérifiant

$$\deg_{Z_0, \dots, Z_n}(f) \leq d, \deg_u(f) \leq \delta$$

Le corps F est comme d'habitude le corps $H(T_1, \dots, T_l)[\eta]$ du chapitre 1.

Dans un premier temps, nous supposons que $F = H$ et que chaque coefficient de f est un paramètre. Alors f est linéaire en les paramètres et le nombre r des paramètres est égale au nombre des coefficients de f en tant que polynôme en Z_0, \dots, Z_n de degré $\leq d$. Le cas général sera étudié dans la sixième section de ce chapitre.

Le polynôme f s'écrit sous la forme

$$f = \sum_{|I| \leq d} u_I Z^I$$

où $I = (i_0, \dots, i_n) \in \mathbb{N}^{n+1}$, $|I| = i_0 + \dots + i_n$ est la norme de I et $Z^I = Z_0^{i_0} \dots Z_n^{i_n}$. Les variables $(u_I)_{|I| \leq d}$ sont les paramètres $u = (u_1, \dots, u_r)$ de f . Alors $r = \binom{n+1+d}{n+1}$ est le nombre des coefficients de f (voir le lemme 6.2.1 de l'appendice).

On pose $\overline{H}_d[Z_0, \dots, Z_n] := \{h \in \overline{H}[Z_0, \dots, Z_n], \deg(h) = d\}$, l'ensemble des polynômes de degrés exactement d en Z_0, \dots, Z_n . Il existe une bijection entre $\overline{H}_d[Z_0, \dots, Z_n]$ et l'ensemble

$$\mathcal{P} = \left(\overline{H}^{\binom{n+d}{n}} \setminus \{(0, \dots, 0)\} \right) \times \overline{H}^{\binom{n+d}{n+1}}$$

qui sera appelé l'espace des paramètres. Le premier facteur correspond aux monômes de degrés d , le second correspond aux monômes de degrés strictement inférieurs à d .

Pour toute spécialisation $a = (a_1, \dots, a_r) \in \mathcal{P}$ des paramètres u_1, \dots, u_r , on note par $f^{(a)} \in \overline{H}[Z_0, \dots, Z_n]$ le polynôme obtenu en remplaçant les u_i par les a_i . Nous nous intéressons dans ce chapitre à la factorisation absolue de $f^{(a)}$ d'une manière uniforme sur les valeurs des paramètres (voir théorème 4.5.1).

Dans la deuxième section nous préparons le polynôme paramétré f aux hypothèses du lemme de Hensel (lemme 4.3.1). Cette préparation se fait par une première décomposition de l'espace des paramètres \mathcal{P} en un nombre fini d'ensembles constructibles chacun avec un changement paramétrique des variables et un polynôme paramétré vérifiant les hypothèses du lemme de Hensel (voir lemme 4.2.1). La troisième section est un rappel d'une version du lemme de Hensel pour les polynômes multivariés. Nous appliquons le lemme de Hensel pour partager de nouveau \mathcal{P} et calculer les facteurs absolument irréductibles de f d'une manière uniforme dans la quatrième et la cinquième section.

4.2 Préparation au lemme de Hensel

L'outil essentiel de ce chapitre est le lemme de Hensel (voir le lemme 4.3.1). Ce lemme ne s'applique que sur les polynômes $g \in F[X, Y_1, \dots, Y_n]$ vérifiant les deux conditions suivantes :

(H1) : $lc_X(g) = 1$, i.e., g est unitaire par rapport à X .

(H2) : $g_0(X) := g(X, 0, \dots, 0)$ est séparable dans $F[X]$.

où $lc_X(g)$ est le coefficient principal de g considéré comme un polynôme univarié en X à coefficients dans $F[Y_1, \dots, Y_n]$.

Pour $a \in \mathcal{P}$, $f^{(a)} \in \overline{H}[Z_0, \dots, Z_n]$ ne vérifie pas nécessairement les conditions (H1) et (H2). Le lemme suivant évite ce problème :

Lemme 4.2.1 *Sous les notations ci-dessus, il existe un algorithme qui décompose l'espace des paramètres \mathcal{P} en*

$$d^{O(n)}$$

ensembles constructibles \mathcal{W} deux à deux disjoints qui vérifient :

1) *Les degrés des équations et des inéquations qui définissent chaque \mathcal{W} sont bornés par $2d$. Leurs tailles binaires sont bornées par $O(nd^2 \log_2(d))$*

2) *Pour tout ensemble \mathcal{W} , ils existent une transformation linéaire des variables X, Y_1, \dots, Y_n et un polynôme $g \in H(u)[X, Y_1, \dots, Y_n]$ (un polynôme à coefficients rationnels en les paramètres). Toute spécialisation des paramètres $a \in \mathcal{W}$ vérifie :*

- *Les dénominateurs des coefficients de g dans $H(u)$ ne s'annulent pas en a .*

- $\deg_u(g) \leq 2d^2$, $\deg_X(g) \leq d$, $\deg_Y(g) \leq 2d^3$ et $l(g) \leq O(nd^3 \log_2(d))$.

- *Le polynôme $g^{(a)} \in \overline{H}[X, Y_1, \dots, Y_n]$ vérifie les conditions (H1) et (H2) ci-dessus, i.e.,*

$$lc_X(g^{(a)}) = 1, \quad g^{(a)}(X, 0, \dots, 0) \text{ est séparable dans } \overline{H}[X].$$

Pour démontrer ce lemme nous aurons besoin de quelques notations et résultats intermédiaires. Tout d'abord, pour des raisons techniques on suppose que $|H| \geq 2d^2$ (dans le cas où $\text{car}(H) = p > 0$). On commence par un lemme connu sous le nom du lemme de Zippel-Schwartz (voir aussi [118, 8]) :

Lemme 4.2.2 *Soit K un corps commutatif et $h \in K[X_1, \dots, X_n]$ un polynôme non nul de degré total d . Alors pour toute famille finie $\{b_0, \dots, b_d\}$ d'éléments deux à deux distincts de K , il existe $(t_1, \dots, t_n) \in \{b_0, \dots, b_d\}^n$ qui vérifie $0 \neq h(t_1, \dots, t_n) \in K$.*

Preuve. Par induction sur n . La propriété est vraie pour $n = 1$ car un polynôme univarié non nul de degré d admet au plus d racines dans K . Supposons que cette propriété est vraie jusqu'à $n - 1$, considérons h comme un polynôme univarié en X_n à coefficients dans $K[X_1, \dots, X_{n-1}]$, l'un de ses coefficients est non nul. Par hypothèse de l'induction, il existe $(t_1, \dots, t_{n-1}) \in \{b_0, \dots, b_d\}^{n-1}$ tel que $h(t_1, \dots, t_{n-1}, X_n)$ est non nul dans $K[X_n]$, de degré $\leq d$. D'où l'existence de $t_n \in \{b_0, \dots, b_d\}$ tel que $h(t_1, \dots, t_n) \neq 0$. \square

A chaque couple (a, T) où $a \in \mathcal{P}$ est une spécialisation des paramètres et T une matrice carrée d'ordre $(n+1)$ à coefficients dans H , on associe le polynôme $g_{(a,T)} \in \overline{H}[X, Y_1, \dots, Y_n]$ défini par

$$g_{(a,T)}(X, Y_1, \dots, Y_n) = f^{(a)}(T(X, Y_1, \dots, Y_n)).$$

Proposition 4.2.3 *On peut produire explicitement une famille $\{T_1, \dots, T_{N_1}\}$ des matrices inversibles d'ordres $(n+1)$ à coefficients dans H . Pour toute valeur $a \in \mathcal{P}$ (i.e., $f^{(a)} \in \overline{H}_d[Z_0, \dots, Z_n]$), il existe $1 \leq i \leq N_1 = (d+1)^n$ tel que le polynôme $g_{(a,T_i)}$ vérifie*

$$0 \neq lc_X(g_{(a,T_i)}) \in \overline{H}.$$

Preuve. Soient $a = (a_I)_{|I| \leq d} \in \mathcal{P}$ et $T = (t_{i,j})_{1 \leq i,j \leq n+1}$ une matrice d'ordre $(n+1)$ à coefficients considérés comme des indéterminés sur H . Alors

$$\begin{aligned} g_{(a,T)}(X, Y_1, \dots, Y_n) &= \sum_{|I| \leq d} a_I \left(t_{1,1}X + t_{1,2}Y_1 + \dots + t_{1,n+1}Y_n \right)^{i_0} \\ &\quad \dots \left(t_{n+1,1}X + t_{n+1,2}Y_1 + \dots + t_{n+1,n+1}Y_n \right)^{i_n} \\ &= \left(\sum_{i_0 + \dots + i_n = |I| = d} a_I t_{1,1}^{i_0} t_{2,1}^{i_1} \dots t_{n+1,1}^{i_n} \right) X^d + G \end{aligned}$$

avec $\deg_X(G) < d$ et

$$0 \neq h := lc_X(g_{(a,T)}) = \sum_{i_0 + \dots + i_n = |I| = d} a_I t_{1,1}^{i_0} t_{2,1}^{i_1} \dots t_{n+1,1}^{i_n} \in \overline{H}[t_{1,1}, t_{2,1}, \dots, t_{n+1,1}]$$

h est un polynôme homogène en $t_{1,1}, t_{2,1}, \dots, t_{n+1,1}$ de degré d . Ce polynôme est non nul car $a \in \mathcal{P}$, i.e., l'un des a_I ($|I| = d$) est non nul.

On fixe $b_0, \dots, b_d \in H$, distincts deux à deux (si $\text{car}(H) = 0$ alors on prend $b_i = i$ et si $\text{car}(H) = p > 0$, on prend $b_i \in \mathbb{F}_{p^m}$ où $p^{m-1} \leq d < p^m$). Par le lemme 4.2.2, il existe $(t_{1,1}, t_{2,1}, \dots, t_{n+1,1}) \in \{b_0, \dots, b_d\}^{(n+1)}$ tel que $h(t_{1,1}, t_{2,1}, \dots, t_{n+1,1}) \neq 0$. Puisque h est homogène alors on peut prendre $t_{1,1} = 1$. En tenant compte de la condition $\det(T) \neq 0$,

on peut prendre

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ t_{2,1} & 1 & 0 & \dots & 0 \\ t_{3,1} & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ t_{n+1,1} & 0 & \dots & 0 & 1 \end{pmatrix}$$

où les coefficients de T sont tous nuls à l'exception de la première colonne et la diagonale principale. Ce qui prouve la proposition en prenant $N_1 = (d+1)^n$. \square

Corollaire 4.2.4 *On peut décomposer l'espace des paramètres \mathcal{P} en $N_1 = (d+1)^n$ ensembles constructibles W_i deux à deux disjoints. Pour chaque W_i , il existe une transformation linéaire inversible T_i et un polynôme paramétré $g_i \in H[u][X, Y_1, \dots, Y_n]$ vérifiant :*

a) $\deg_u(g_i) = 1$, $\deg_X(g_i) = d$, $\deg_Y(g_i) \leq d$. Sa taille binaire est $l(g_i) \leq d \log_2(d)$.

b) Pour tout $a \in W_i$, $0 \neq lc_X(g_i^{(a)}) \in \overline{H}$.

Cette partition se fait avec $(d+1)^{2n+1}$ opérations dans H . Sa complexité binaire est $(d+1)^{2n+1} \log_2(d)$.

Preuve. Pour chaque matrice T_i ($1 \leq i \leq N_1$) du proposition 4.2.3, considérons les polynômes suivants :

$$g_i := g_{(u, T_i)} \in H[u][X, Y_1, \dots, Y_n] \quad \text{et} \quad h_i := lc_X(g_i) \in H[u].$$

Prenons W_i l'ensemble constructible défini par les équations et les inéquations suivantes :

$$h_1 = 0, \dots, h_{i-1} = 0, h_i \neq 0.$$

La taille binaire de chaque coefficient de T_i est bornée par $\log_2(d)$ (voir la preuve du proposition 4.2.3). La complexité de cette partition est égale à celle du calcul des polynômes g_1, \dots, g_{N_1} où

$$g_i = f(X, t_{2,1}X + Y_1, \dots, t_{n+1,1}X + Y_n).$$

Ce qui prouve le corollaire par le lemme 6.1.5 de l'appendice. \square

Par une division de chaque g_i par son coefficient principal h_i on obtient un polynôme de $H(u)[X, Y_1, \dots, Y_n]$ qui vérifie la condition (H1) ci-dessus pour toute spécialisation $a \in W_i$. Nous procédons maintenant à la démonstration du lemme 4.2.1.

Preuve du lemme 4.2.1 :

Pour assurer la séparabilité (i.e., la condition (H2)), nous fixons un triplet (W_i, g_i, h_i) du corollaire 4.2.4. Pour tout $a \in W_i$, il existe un exposant t tel que p^t est la plus grande puissance qui divise tous les exposants de X dans le polynôme $\frac{1}{h_i^{(a)}} g_i^{(a)} \in \overline{H}[X, Y_1, \dots, Y_n]$.

Pour tout $0 \leq t \leq \lfloor \frac{\log_2 d}{\log_2 p} \rfloor$ (où $\lfloor * \rfloor$ est la partie entière de $*$), considérons le polynôme $g_{i,t} \in H(u)[X, Y_1, \dots, Y_n]$ défini par :

$$\frac{1}{h_i} g_i(X, Y_1, \dots, Y_n) = g_{i,t}(X^{p^t}, Y_1, \dots, Y_n)$$

et le sous-ensemble constructible $W_{i,t}$ défini dans W_i par l'inéquation :

$$\frac{\partial}{\partial X}(g_{i,t}) \neq 0 \quad (4.1)$$

Alors

$$W_i = \bigcup_{0 \leq t \leq \lfloor \frac{\log_2 d}{\log_2 p} \rfloor} W_{i,t}$$

et pour tout $a \in W_{i,t}$, le polynôme $g_{i,t}^{(a)} \in \overline{H}[X, Y_1, \dots, Y_n]$ vérifie :

- Les degrés des coefficients de $g_{i,t}$ par rapport à u sont égaux à 1.
- $g_{i,t}^{(a)}$ est unitaire par rapport à X
- $\frac{\partial}{\partial X}(g_{i,t}^{(a)}) \neq 0$, $\deg_X(g_{i,t}^{(a)}) = dp^{-t}$, $\deg_Y(g_{i,t}^{(a)}) \leq d$.

Si $\text{car}(F) = 0$, on obtient $W_i = W_{i,0}$ qui est défini par (4.1) avec la convention $0^0 = 1$.

Fixons un ensemble $W_{i,t}$ et calculons le discriminant suivant :

$$Dis := Disc_X(g_{i,t}) = \text{res}_X \left(g_{i,t}, \frac{\partial}{\partial X}(g_{i,t}) \right) \in H(u)[Y_1, \dots, Y_n]$$

Ce polynôme vérifie (voir le lemme 6.2.3 de l'appendice) :

- $\deg_Y(Dis) \leq d(2dp^{-t} - 1) =: D_1$.
- Les degrés de ses coefficients par rapport à u sont bornés par $2dp^{-t} - 1 \leq 2d$.
- La taille binaire de Dis est $l(Dis) \leq 2d^2 \log_2(d)$.

Considérons les deux ensembles suivants :

$$W_{i,t}^{(1)} = \{a \in W_{i,t}, 0 \equiv Dis^{(a)} \in \overline{H}[Y_1, \dots, Y_n]\}, \quad W_{i,t}^{(2)} = \{a \in W_{i,t}, 0 \neq Dis^{(a)}\}$$

alors

$$W_{i,t} = W_{i,t}^{(1)} \cup W_{i,t}^{(2)}$$

On commence à décomposer $W_{i,t}^{(2)}$, pour cela on fixe $b_0, \dots, b_{D_1} \in H$ deux à deux distincts (si $\text{car}(F) = p > 0$, on prend $b_i \in \mathbb{F}_{p^m}$ où $p^{m-1} \leq D_1 < p^m$). Pour chaque $a \in W_{i,t}^{(2)}$, le lemme 4.2.2 montre qu'il existe $c^{(j)} = (c_1^{(j)}, \dots, c_n^{(j)}) \in \{b_0, \dots, b_{D_1}\}^n$ qui vérifie

$0 \neq \text{Dis}^{(a)}(c^{(j)}) \in \overline{H}$. Alors $g_{i,t}^{(a)}(X, c_1^{(j)}, \dots, c_n^{(j)})$ est séparable dans $\overline{H}[X]$.

Pour tout $1 \leq j \leq N_2 = (D_1 + 1)^n$, considérons le polynôme

$$g_{i,t,j}(X, Y_1, \dots, Y_n) = g_{i,t}(X, Y_1 + c_1^{(j)}, \dots, Y_n + c_n^{(j)}) \in H(u)[X, Y_1, \dots, Y_n]$$

et le sous-ensemble constructible $W_{i,t}^{(2,j)}$ défini dans $W_{i,t}^{(2)}$ par l'inéquation :

$$\text{Dis}(c^{(j)}) \neq 0$$

où $\text{Dis}(c^{(j)}) \in H(u)$ est de degré borné par $2d$ et de taille binaire $\leq O(d^2 \log_2(d))$. Alors

$$W_{i,t}^{(2)} = \bigcup_{1 \leq j \leq N_2} W_{i,t}^{(2,j)}$$

Pour tout $a \in W_{i,t}^{(2)}$, le polynôme $g_{i,t,j}^{(a)}(X, Y_1, \dots, Y_n) \in \overline{H}[X, Y_1, \dots, Y_n]$ vérifie :

- Les degrés des coefficients de $g_{i,t,j}$ par rapport à u sont égaux à 1.
- $\deg_X(g_{i,t,j}) = dp^{-t}$, $\deg_Y(g_{i,t,j}) \leq d$ et $l(g_{i,t,j}) \leq O(d \log_2(d))$.
- $g_{i,t,j}^{(a)}$ est unitaire par rapport à X (i.e., la condition (H1)).
- $g_{i,t,j}^{(a)}(X, 0, \dots, 0)$ est séparable dans $\overline{H}[X]$ (i.e., la condition (H2)).

Pour décomposer $W_{i,t}^{(1)}$, on considère les deux polynômes univariés $P := g_{i,t}$, $Q = \frac{\partial}{\partial X}(g_{i,t}) \in K[X]$ où $K = H(u)[Y_1, \dots, Y_n]$. Calculons la suite signée suivante des sous-resultants de P et Q :

$$SR_{dp^{-t}}, SR_{dp^{-t}-1}, \dots, SR_1, SR_0 \in K[X]$$

par l'algorithme 8.73 de [8].

Pour tout $a \in W_{i,t}^{(1)}$, les dénominateurs des coefficients de cette suite ne s'annulent pas en a . Puisque $\deg_X(P^{(a)}) = \deg_X(P)$ et $\deg_X(Q^{(a)}) = \deg_X(Q)$ (P est unitaire en X) alors la suite signée des sous-resultants de $P^{(a)}$ et $Q^{(a)}$ est :

$$SR_{dp^{-t}}^{(a)}, SR_{dp^{-t}-1}^{(a)}, \dots, SR_1^{(a)}, SR_0^{(a)} \in \overline{H}[Y_1, \dots, Y_n][X]$$

(proposition 8.71 de [8]).

Puisque $\deg_u(P) = \deg_u(Q) = 1$ et $\deg_Y(P), \deg_Y(Q) \leq d$, les propositions 8.68 et 8.69 de [8] montrent que :

$$\deg_u SR_j \leq 2d, \quad \deg_Y SR_j \leq 2d^2, \quad l(SR_j) \leq O(nd^2 \log_2(d)), \quad 0 \leq j \leq dp^{-t}.$$

Ecrivons SR_j sous la forme

$$SR_j = A_j^{(j)} X^j + \dots + A_0^{(j)}$$

où $A_k^{(j)} \in H(u)[Y_1, \dots, Y_n]$ et $\deg_Y A_k^{(j)} \leq 2d^2$. Pour tout $1 \leq j \leq dp^{-t}$, soit le sous-ensemble constructible $W_{i,t}^{(1,j)}$ de $W_{i,t}^{(1)}$ défini par les équations et les inéquations suivantes :

$$A_1^{(1)} = 0, \dots, A_{j-1}^{(j-1)} = 0, A_j^{(j)} \neq 0.$$

En tenant compte du corollaire 8.55 de [8], pour tout $a \in W_{i,t}^{(1,j)}$, $SR_j^{(a)} \in \overline{H}[Y_1, \dots, Y_n][X]$ est un p.g.c.d. de $P^{(a)}$ et $Q^{(a)}$ de degré j en X .

En plus par cette construction on obtient la partition suivante :

$$W_{i,t}^{(1)} = \bigcup_{1 \leq j \leq dp^{-t}-1} W_{i,t}^{(1,j)}.$$

Soit $b = A_j^{(j)} \in H(u)[Y_1, \dots, Y_n]$ et m le premier entier pair plus grand que $dp^{-t} - j + 1$. Par la division Euclidienne de $b^m g_{i,t}$ par SR_j , on calcule deux polynômes $Q_j, R_j \in H(u)[Y_1, \dots, Y_n][X]$ avec

$$b^m g_{i,t} = SR_j Q_j + R_j, \quad \deg_X R_j < j$$

(En d'autres termes, effectuons la pseudo-division de $g_{i,t}$ par SR_j dans $K[X]$).

Pour tout $a \in W_{i,t}^{(1,j)}$, $R_j^{(a)} = 0$ et le polynôme $Q_j^{(a)} \in \overline{H}[X, Y_1, \dots, Y_n]$ vérifie :

- Les degrés des coefficients de Q_j par rapport à u sont bornés par $2d^2$.
- $Q_j^{(a)}$ est unitaire par rapport à X (i.e., la condition (H1)).
- $Q_j^{(a)}(X, 0, \dots, 0)$ est séparable dans $\overline{F}[X]$ (i.e., la condition (H2)).
- $\deg_X(Q_j^{(a)}) = dp^{-t} - j$, $\deg_Y(Q_j^{(a)}) \leq 2d^3$ et $l(Q_j) \leq O(nd^3 \log_2(d))$.

Il reste à estimer le nombre M_1 des ensembles constructibles obtenus par la partition préparatoire de l'espace des paramètres :

$$\begin{aligned} M_1 &\leq N_1 \lfloor \frac{\log_2 d}{\log_2 p} \rfloor (N_2 + d) \\ &\leq (d+1)^n d \left((2d^2 + 1)^n + d \right) \\ &\leq d^{O(n)}. \square \end{aligned}$$

Corollaire 4.2.5 *L'algorithme du lemme 4.2.1 se fait avec*

$$d^{O(n)}$$

opérations dans H . Sa complexité binaire est

$$d^{O(n)} \log_2^2(d).$$

Preuve. Dans la preuve du lemme 4.2.1, le calcul du discriminant Dis se fait avec $O((2dp^{-t} - 1)^{2.376}) \leq O(d^{2.376})$ opérations dans $H(u)[Y_1, \dots, Y_n]$ [29]. Chacune de ces opérations se fait entre deux éléments de $H(u)[Y_1, \dots, Y_n]$ de degrés $\leq (d+1)(2dp^{-t} - 1) \leq 4d^2$ en (u, Y_1, \dots, Y_n) , et des tailles binaires $\leq O(d^2 \log_2(d))$. Donc le calcul de Dis se fait avec

$$O(d^{2.376})d^{O(n)} \leq d^{O(n)}$$

opérations dans H . Sa complexité binaire est bornée par $d^{O(n)} \log_2^2(d)$.

La construction de tous les $W_{i,t}^{(2,j)}$ coûte

$$N_2 \binom{n + D_1}{n} \leq d^{O(n)}$$

opérations dans H . Sa complexité binaire est bornée par $d^{O(n)} \log_2^2(d)$.

Le calcul de la suite signée des sous-resultants de P et Q se fait avec $O(dp^{-t}(dp^{-t} - 1)) = O(d^2)$ opérations dans K (Voir Algorithme 8.73 de [8]). Chacune de ces opérations se fait avec $d^{O(n)}$ opérations dans H . Le calcul de la suite signée des sous-resultants se fait donc en utilisant $d^{O(n)}$ opérations dans H . Sa complexité binaire est bornée par $d^{O(n)} \log_2^2(d)$.

La division Euclidienne de $b^m g_{i,t}$ par SR_j se fait par $(dp^{-t} - j + 1)(2j + 3) = O(d^2)$ opérations dans K (Algorithme 8.6 de [8]). Donc cette division se fait avec $d^{O(n)}$ opérations dans H . Sa complexité binaire est bornée par $d^{O(n)} \log_2^2(d)$. \square

4.3 Lemme de Hensel

Nous rappelons dans cette section le lemme de Hensel (voir [126, 103, 102, 22, 58, 96, 118]).

Lemme 4.3.1 *Soit $R_N = F[Y_1, \dots, Y_n]/((Y_1, \dots, Y_n)^N)$, où $1 \leq N < \infty$, et $R_\infty = F[Y_1, \dots, Y_n]$.*

Soit $N > 1$ et $g \in R_N[X]$ vérifiant les propriétés suivantes :

$$(H1) \quad lc_X(g) = 1.$$

$$(H2) \quad g_0(X) = g(X, 0, \dots, 0) \text{ est séparable dans } F[X].$$

Alors pour toute décomposition de g_0 sous la forme $g_0 = g_0^{(1)} \cdots g_0^{(s)}$ où $g_0^{(1)}, \dots, g_0^{(s)} \in F[X]$ sont unitaires on a :

Pour tout multi-indice $I = (i_1, \dots, i_n)$, $|I| > N \geq 1$, il existe des polynômes uniques $g_I^{(1)}, \dots, g_I^{(s)} \in F[X]$ qui vérifient :

$$i) \deg(g_I^{(j)}) < \deg(g_0^{(j)}), \quad |I| \geq 1, \quad 1 \leq j \leq s.$$

ii) Dans la complétion de $R_N[X]$ en respectant (Y_1, \dots, Y_n) nous avons la décomposition suivante :

$$g = G_1 \cdots G_s, \quad \text{où } G_j = g_0^{(j)} + \sum_{|I| \geq 1} g_I^{(j)} Y^I, \quad 1 \leq j \leq s.$$

Pour $N' < N$ la décomposition ii) de l'image de g par l'homomorphisme naturel $\nu : R_N[X] \rightarrow R_{N'}[X]$ est obtenue en appliquant ν .

Pour prouver le lemme de Hensel nous aurons besoin du lemme suivant [118] :

Lemme 4.3.2 Soit K un corps commutatif et $f, g, h \in K[X]$ trois polynômes univariés tels que f et g sont premiers entre eux et $\deg(h) < \deg(f) + \deg(g)$. Alors il existe de polynômes uniques $u, v \in K[X]$ tels que

$$uf + vg = h$$

et

$$\deg(u) < \deg(g), \deg(v) < \deg(f).$$

Preuve. Par l'égalité de Bézout, ils existent $\tilde{u}, \tilde{v} \in K[X]$ tel que $\tilde{u}f + \tilde{v}g = 1$. Alors $(h\tilde{u})f + (h\tilde{v})g = h$. Effectuons la division Euclidienne de $h\tilde{u}$ par g , ils existent $q, u \in K[X]$ tels que $h\tilde{u} = qg + u$ et $\deg(u) < \deg(g)$. Donc

$$uf + (qf + h\tilde{v})g = h$$

ce qui prouve l'existence de u et $v := qf + h\tilde{v}$. Puisque $vg = h - uf$ alors $\deg(vg) \leq \deg(h) < \deg(f) + \deg(g)$, ce qui prouve que $\deg(v) < \deg(f)$. S'ils existent $u', v' \in K[X]$ tels que $u'f + v'g = h$ et $\deg(u') < \deg(g)$, $\deg(v') < \deg(f)$ alors

$$(u - u')f + (v - v')g = 0$$

donc g divise $(u - u')$ car g est premier avec f , mais $\deg(u - u') < \deg(g)$ alors $u - u' = 0$ et par suite $v - v' = 0$. Ce qui prouve l'unicité et le lemme. \square

Preuve du lemme 4.3.1

Ecrivons g sous la forme $g = g_0 + \sum_{|I| \geq 1} g_I Y^I$ où $g_I \in F[X]$, $\deg(g_I) < \deg(g_0)$ car $lc_X(g) = 1$. Nous allons montrer ce lemme par récurrence sur s . Commençons par le cas $s = 2$:

Existence : L'égalité $g = G_1 G_2$ dans ii) est équivalente à :

$$g_0^{(1)} g_I^{(2)} + g_0^{(2)} g_I^{(1)} = h_I \quad \text{pour tout } |I| \geq 1 \quad (4.2)$$

où

$$h_I := g_I - \sum_{1 \leq |J| < |I|} g_J^{(1)} g_{I-J}^{(2)}$$

Supposons que pour tout $|J| < |I|$, $g_J^{(1)}$, $g_J^{(2)}$ existent et vérifient la condition i). Donc h_I est construit et $\deg(h_I) < \deg(g_0^{(1)}) + \deg(g_0^{(2)})$. Puisque g_0 est séparable alors $g_0^{(1)}$ et $g_0^{(2)}$ sont premiers entre eux, ce qui prouve l'existence de $g_I^{(1)}$ et $g_I^{(2)}$ vérifiant i) par application du lemme 4.3.2.

Unicité : S'ils existent de polynômes $g_I^{(1)}, g_I^{(2)} \in F[X]$, $|I| \geq 1$ qui vérifient les conditions i) et ii) du lemme, alors ils vérifient les égalités (4.2). Ce qui prouve leurs unicités par le lemme 4.3.2.

Supposons que cette propriété est vraie jusqu'à $s - 1$ et démontrons-la pour s . Posons $h_0 := g_0^{(2)} \cdots g_0^{(s)}$ alors $g_0 = g_0^{(1)} h_0$ vérifie les conditions (H1) et (H2) ci-dessus. Par l'hypothèse de récurrence, il existe de polynômes uniques $g_I^{(1)}, \tilde{g}_I^{(2)} \in F[X]$ tels que

$$\deg(g_I^{(1)}) < \deg(g_0^{(1)}), \quad \deg(\tilde{g}_I^{(2)}) < \deg(h_0)$$

et

$$g = G_1 \tilde{G}_2 \quad \text{où} \quad \tilde{G}_2 := h_0 + \sum_{|I| \geq 1} \tilde{g}_I^{(2)} Y^I$$

\tilde{G}_2 est unitaire par rapport à X (i.e., vérifie la condition (H1)) et $\tilde{G}_2(X, 0, \dots, 0) = h_0$ se décompose en produit de $(s - 1)$ facteurs vérifiant la condition (H2). Ce qui prouve le lemme par application de l'hypothèse de récurrence pour $(s - 1)$. \square

Sous les hypothèses du lemme de Hensel, une généralisation des égalités (4.2) au cas $s \geq 2$ est donnée par les équations suivantes qui sont équivalentes au condition ii) du lemme 4.3.1 :

$$g_I = \sum_{\cup_{0 \leq l \leq s} J_l = I} \prod_{0 \leq k \leq s} g_{J_k}^{(k)}, \quad |I| \geq 1.$$

Alors

$$g_I = \sum_{1 \leq j \leq s} g_0^{(1)} \cdots g_0^{(j-1)} g_I^{(j)} g_0^{(j+1)} \cdots g_0^{(s)} + V_I, \quad |I| \geq 1. \quad (4.3)$$

où V_I dépend seulement des polynômes $g_J^{(1)}, \dots, g_J^{(s)} \quad |J| < |I|$.

Soit $\mathcal{D} := \deg_X(g) = \deg(g_0)$. Pour $|I|$ fixé, les coefficients de $g_I^{(1)}, \dots, g_I^{(s)}$ forment un vecteur de $F^{\mathcal{D}}$ qui est la solution unique du système linéaire $Bx = b_I$ obtenu par (4.3), où B est une matrice carré d'ordre \mathcal{D} dont ses entrées dépendent seulement des coefficients de $g_0^{(1)}, \dots, g_0^{(s)}$ (B est inversible par l'unicité de $g_I^{(1)}, \dots, g_I^{(s)}$ dans le lemme 4.3.1). Le second membre b_I dépend des coefficients de g_I et V_I .

Remarque 4.3.3 Dans le cas $s = 2$, on obtient que $B = \text{Sylv}(g_0^{(1)}, g_0^{(2)})$ est la matrice de Sylvester de $g_0^{(1)}$ et $g_0^{(2)}$.

Notations : Pour tout $1 \leq j \leq s$, soit $k_j = \deg(g_0^{(j)})$ alors $\mathcal{D} = \sum_j k_j$. Posons

$$g_0^{(j)} = X^{k_j} + \sum_{0 \leq i < k_j} \alpha_i^{(j)} X^i, \quad g_I^{(j)} = \sum_{0 \leq i < k_j} \alpha_i^{(j,I)} X^i$$

et

$$g_I = \sum_{0 \leq i < \mathcal{D}} v_{i,I} X^i, \quad |I| \geq 1.$$

Théorème 4.3.4 *Sous les hypothèses du lemme 4.3.1 et les notations ci-dessus, pour tout $|I| \geq 1$, les coefficients de $g_I^{(1)}, \dots, g_I^{(s)}$ sont des fonctions rationnelles des coefficients de $g_0^{(1)}, \dots, g_0^{(s)}$ et des coefficients de g et sont donnés par :*

$$\alpha_i^{(j,I)} = \frac{P_i^{(j,I)}}{(\det(B))^{2|I|-1}}, \quad 1 \leq j \leq s, \quad 0 \leq i < k_j.$$

où $P_i^{(j,I)}$ est un polynôme dont ses variables sont les coefficients de $g_0^{(1)}, \dots, g_0^{(s)}$ et les coefficients de g considérés comme des indéterminés sur H . Ses coefficients sont des éléments de H . En plus,

a) Les degrés par rapport aux coefficients de $g_0^{(1)}, \dots, g_0^{(s)}$ et ceux de g sont donnés par

$$\deg_{\alpha_i^{(j)}}(P_i^{(j,I)}) \leq (2|I| - 1)(\mathcal{D} - 1)(s - 1), \quad \deg_{\alpha_i^{(j)}}(\det(B)) \leq (\mathcal{D} - 1)(s - 1)$$

et

$$\deg_{v_{i,I}}(P_i^{(j,I)}) \leq (2|I| - 1)(s - 1).$$

b) Si $F = H$ et M est une borne supérieure de taille binaire de g alors celle de $P_i^{(j,I)}$ est bornée par

$$sM + (2|I| - 1)(\mathcal{D} - 1)(s - 1).$$

Preuve.

On donne la preuve dans le cas $s = 2$, le cas général est analogue.

Pour $s = 2$, on démontre le théorème par récurrence sur $|I|$:

Pour $|I| = 1$, écrivons les formules de *Cramer* du système linéaire $Bx = b_I$:

$$\alpha_i^{(j,I)} = \frac{\det(\Delta)}{\det(B)}$$

où Δ est la matrice obtenue à partir de B en remplaçant une certaine colonne (qui correspond à j, i) par le vecteur b_I qui est formé dans ce cas des coefficients $v_{i,I}$ de g_I seulement.

Le polynôme $P_i^{(j,I)} := \det(\Delta)$ vérifie les bornes sur les degrés et la taille binaire du théorème.

Supposons que les conditions a) et b) du théorème sont vérifiées pour tout multi-indice J tel que $|J| < |I|$ et montrons-les pour I . Les entrées du vecteur b_I sont donnés par :

$$b_{\mathcal{D}-1} = v_{\mathcal{D}-1,I} \quad \text{et} \quad b_k = v_{k,I} - \sum_{1 \leq |J| < |I|} \sum_{0 \leq l \leq k} \alpha_l^{(1,J)} \alpha_{k-l}^{(2,I-J)}, \quad 0 \leq k \leq \mathcal{D}-2$$

En utilisant l'hypothèse de récurrence on obtient :

$$b_k = \frac{1}{(\det(B))^{2|I|-2}} \left(v_{k,I} (\det(B))^{2|I|-2} - \sum_{1 \leq |J| < |I|} \sum_{0 \leq l \leq k} P_l^{(1,J)} P_{k-l}^{(2,I-J)} \right).$$

De nouveau les formules de *Cramer* nous donnent $\alpha_i^{(j,I)} = \frac{\det(\Delta)}{\det(B)}$, on développe $\det(\Delta)$ suivant le vecteur b_I :

$$\begin{aligned} \det(\Delta) &= \sum_{0 \leq k \leq \mathcal{D}-1} (-1)^{\epsilon_k} b_k \det(B_k) = (-1)^{\epsilon_{\mathcal{D}-1}} v_{\mathcal{D}-1,I} \det(B_{\mathcal{D}-1}) \\ &+ \frac{1}{(\det(B))^{2|I|-2}} \sum_{0 \leq k \leq \mathcal{D}-2} (-1)^{\epsilon_k} \left(v_{k,I} (\det(B))^{2|I|-2} - \sum_{1 \leq |J| < |I|} \sum_{0 \leq l \leq k} P_l^{(1,J)} P_{k-l}^{(2,I-J)} \right) \det(B_k) \end{aligned}$$

où chaque B_k est une sous-matrice de B d'ordre $\mathcal{D}-1$. Donc on peut écrire chaque $\alpha_i^{(j,I)}$ sous la forme :

$$\alpha_i^{(j,I)} = \frac{P_i^{(j,I)}}{(\det(B))^{2|I|-1}}$$

avec

$$\begin{aligned} \deg_{\alpha_i^{(j)}}(P_i^{(j,I)}) &\leq \max \{ (2|I| - 2 + 1)(\mathcal{D} - 1), (2|J| - 1)(\mathcal{D} - 1) + (2|I - J| - 1)(\mathcal{D} - 1) + (\mathcal{D} - 1) \} \\ &\leq (2|I| - 1)(\mathcal{D} - 1) \end{aligned}$$

et

$$\begin{aligned} \deg_{v_{i,I}}(P_i^{(j,I)}) &\leq \max \{ 1, (2|J| - 1) + (2|I - J| - 1) \} \\ &\leq (2|I| - 1). \end{aligned}$$

Sa taille binaire est donnée par

$$\begin{aligned} l(P_i^{(j,I)}) &\leq \max \{ M + (2|I| - 2 + 1)(\mathcal{D} - 1), 2M + (2|I| - 1)(\mathcal{D} - 1) \} \\ &\leq 2M + (2|I| - 1)(\mathcal{D} - 1). \square \end{aligned}$$

4.4 Partition de l'espace des paramètres par le lemme de Hensel

Revenons au résultat du lemme 4.2.1 et fixons un couple (\mathcal{W}, g) où \mathcal{W} est un ensemble constructible, g est un polynôme paramétré, i.e., $g \in H(u)[X, Y_1, \dots, Y_n]$. Toute spécialisation des paramètres $a \in \mathcal{W}$ vérifie :

$$lc_X(g^{(a)}) = 1, \quad g^{(a)}(X, 0, \dots, 0) \text{ est séparable dans } \overline{H}[X].$$

(i.e., $g^{(a)}$ satisfait les conditions (H1) et (H2) du lemme 4.3.1).

Soit $\mathcal{D} := \deg_X(g) \leq d$, $\deg_Y(g) \leq 2d^3$ (voir lemme 4.2.1). On écrit g sous la forme :

$$g = X^{\mathcal{D}} + \sum_{0 \leq |I| \leq 2d^3, 0 \leq i < \mathcal{D}} v_{i,I} X^i Y^I = g_0 + \sum_{1 \leq |I| \leq 2d^3} g_I Y^I$$

où $v_{i,I} \in H(u)$. Soit $k = (k_1, \dots, k_s) \in \mathbb{N}^s$ une partition de \mathcal{D} , c'est à dire $\mathcal{D} = k_1 + \dots + k_s$, $k_1 \geq \dots \geq k_s$, on associe à cette partition un sous-ensemble U_k de \mathcal{W} défini par :

Définition 4.4.1 U_k est l'ensemble des valeurs $a \in \mathcal{W}$ des paramètres tel que le polynôme associé $g^{(a)}$ vérifie la condition suivante :

(H3) : ils existent des polynômes unitaires $g_0^{(1)}, \dots, g_0^{(s)} \in \overline{H}[X]$ qui vérifient

$$g_0^{(a)} = g_0^{(1)} \cdots g_0^{(s)}, \quad \deg(g_0^{(j)}) = k_j, \quad 1 \leq j \leq s$$

et tel que par application du lemme 4.3.1 on obtient une factorisation de $g^{(a)}$ dans $\overline{H}[X, Y_1, \dots, Y_n]$. En d'autres termes les $G_j^{(a)}$ ($1 \leq j \leq s$) donnés par le lemme 4.3.1 sont dans $\overline{H}[X, Y_1, \dots, Y_n]$. Cette condition sera appelée la condition de terminaison.

Ecrivons les fonctions rationnelles $v_{i,I}$ (coefficients de g) sous la forme :

$$v_{i,I} = \frac{S_{i,I}}{R_{i,I}} \quad \text{où} \quad S_{i,I}, R_{i,I} \in H[u]$$

avec $R_{i,I}^{(a)} \neq 0$ pour tout $a \in \mathcal{W}$.

La condition $g_0^{(a)} = g_0^{(1)} \cdots g_0^{(s)}$ est équivalente à :

$$S_{i,0}^{(a)} = R_{i,0}^{(a)} \sum_{0=l_0 \leq l_1 \leq \dots \leq l_s=i} \prod_{1 \leq m \leq s} \alpha_{l_m - l_{m-1}}^{(m)}, \quad 0 \leq i < \mathcal{D} \quad (4.4)$$

où $\alpha_{k_j}^{(j)} = 1$, $1 \leq j \leq s$ et les $\alpha_i^{(j)}$ sont les coefficients de $g_0^{(j)}$ (comme dans la section précédente).

Rappelons que chaque G_j est écrit dans le lemme 4.3.1 sous la forme :

$$G_j = g_0^{(j)} + \sum_{|I| \geq 1} g_I^{(j)} Y^I$$

Les coefficients de $g_I^{(j)}$ forment la solution unique d'un certain système linéaire $Bx = b_I$ (voir la section précédente). Nous allons établir dans la suite une condition équivalente à la condition de terminaison.

Lemme 4.4.2 *Soit I un multi-indice, $|I| > 2d^3$. Alors $g_I^{(j)} = 0$ pour tout $1 \leq j \leq s$ si et seulement si $V_I = 0$ (où V_I est donné par (4.3)).*

Preuve. Puisque $g_I = 0$ (car $\deg_Y(g) \leq 2d^3$). Alors $V_I = 0$ si et seulement si le second membre b_I du système linéaire $Bx = b_I$ est nul, ceci est équivalent à que ce système admet 0 comme solution unique, ce qui prouve le lemme. \square

Théorème 4.4.3 *La condition de terminaison est équivalente à que*

$$V_I = 0, \quad 2d^3 < |I| \leq 2sd^3.$$

Preuve.

La condition de terminaison est équivalente à que $\deg_Y(G_j) \leq 2d^3$ pour tout $1 \leq j \leq s$, donc à $g_I^{(j)} = 0$ pour tout $1 \leq j \leq s$ et $|I| > 2d^3$. Par le lemme 4.4.2, ces conditions sont équivalentes à que $V_I = 0$ pour tout $|I| > 2d^3$. Nous faisons la preuve dans le cas $s = 2$, le cas général se fait d'une manière analogue. Nous avons

$$V_I = \sum_{1 \leq |J| < |I|} g_J^{(1)} g_{I-J}^{(2)}$$

La seule chose qu'il faut montrer est que $V_I = 0$ pour tout $2d^3 < |I| \leq 4d^3$ implique $V_I = 0$ pour tout $|I| > 2d^3$. Le lemme 4.4.2 montre que $g_I^{(1)} = g_I^{(2)} = 0$ pour tout $2d^3 < |I| \leq 4d^3$, montrons par récurrence sur t que $V_I = 0$ pour $|I| = 2d^3 + t$ et tout $t \geq 2d^3 + 1$. En effet pour $t = 2d^3 + 1$ (i.e., $|I| = 4d^3 + 1$). On décompose V_I en deux sommes :

$$V_I = \sum_{1 \leq |J| \leq 2d^3} g_J^{(1)} g_{I-J}^{(2)} + \sum_{2d^3 < |J| \leq 4d^3} g_J^{(1)} g_{I-J}^{(2)}$$

Pour $2d^3 < |J| \leq 4d^3$, $g_J^{(1)} = 0$ alors la seconde quantité est nulle et pour $1 \leq |J| \leq 2d^3$ on obtient $2d^3 < |I - J| \leq 4d^3$ et $g_{I-J}^{(2)} = 0$ et donc la première quantité est nulle, d'où $V_I = 0$. Supposons maintenant que $V_I = 0$ pour $2d^3 < |I| \leq 2d^3 + t$ et $t \geq 2d^3 + 1$. Alors pour $|I| = 2d^3 + t + 1$ on a :

$$V_I = \sum_{1 \leq |J| \leq 2d^3} g_J^{(1)} g_{I-J}^{(2)} + \sum_{2d^3 < |J| \leq 2d^3 + t} g_J^{(1)} g_{I-J}^{(2)}$$

pour $2d^3 < |J| \leq 2d^3 + t$, on obtient $g_J^{(1)} = 0$ (hypothèse de récurrence) et pour $1 \leq |J| \leq 2d^3$ on obtient $2d^3 < |I - J| \leq 2d^3 + t$ et $g_{I-J}^{(2)} = 0$, donc $V_I = 0$. \square

Nous donnons les équations sur les paramètres qui sont équivalentes à la condition de terminaison du théorème 4.4.3. Chaque polynôme $V_I \in H(\alpha_i^{(j)}, u)[X]$ donné par (4.3) dépend seulement des polynômes $\{g_J^{(j)}\}_{|J| < |I|, 1 \leq j \leq s}$. Remplaçons les coefficients des polynômes $\{g_J^{(j)}\}_{1 \leq |J| \leq 2sd^3, 1 \leq j \leq s}$ dans les conditions de terminaison $V_I = 0$, $2d^3 < |I| \leq 2sd^3$ par leurs expressions données par le théorème 4.3.4, on obtient des équations polynomiales de la forme :

$$Q_i^{(I)} = 0, \quad 2d^3 < |I| \leq 2sd^3, \quad 0 \leq i \leq \mathcal{D} - 2 \quad (4.5)$$

où chaque $Q_i^{(I)} \in H[\alpha_i^{(j)}, u]$, les $\alpha_i^{(j)}$ sont les coefficients de $g_0^{(j)}$.

Les degrés de ces équations par rapport aux paramètres u et par rapport aux $\alpha_i^{(j)}$ sont donnés par le corollaire suivant :

Corollaire 4.4.4 *Pour tout $2d^3 < |I| \leq 2sd^3$, $0 \leq i \leq \mathcal{D} - 2$ on a :*

$$\begin{aligned} \deg_{\alpha_i^{(j)}}(Q_i^{(I)}) &\leq 2(|I| - 1)(\mathcal{D} - 1)(s - 1) \\ &\leq 2(2sd^3 - 1)(\mathcal{D} - 1)(s - 1) \end{aligned}$$

et

$$\begin{aligned} \deg_u(Q_i^{(I)}) &\leq 4d^2(|I| - 1)(s - 1) \\ &\leq 4d^2(2sd^3 - 1)(s - 1) \end{aligned}$$

Preuve. (cas $s = 2$)

$$Q_i^{(I)} = \sum_{1 \leq |J| < |I|, 0 \leq l \leq i} P_l^{(1,J)} P_{i-l}^{(2,I-J)}$$

En utilisant les bornes des degrés dans le théorème 4.3.4 on obtient

$$\begin{aligned} \deg_{\alpha_i^{(j)}}(Q_i^{(I)}) &\leq (2|J| - 1)(\mathcal{D} - 1) + (2|I - J| - 1)(\mathcal{D} - 1) \\ &= 2(|I| - 1)(\mathcal{D} - 1). \end{aligned}$$

et

$$\begin{aligned} \deg_{v_{i,I}}(Q_i^{(I)}) &\leq (2|J| - 1) + (2|I - J| - 1) \\ &= 2(|I| - 1) \end{aligned}$$

En tenant compte aussi que $\deg_u(g)$ et donc $\deg(v_{i,I})$ sont bornés par $2d^2$ (lemme 4.2.1) on obtient

$$\deg_u(Q_i^{(I)}) \leq 4d^2(|I| - 1). \square$$

Corollaire 4.4.5 Soit $k = (k_1, \dots, k_s)$, $s \geq 2$ une partition de \mathcal{D} . Alors l'ensemble U_k est la \overline{H} -réalisation dans \mathcal{W} de la formule quantifiée suivante :

$$\exists \alpha_i^{(j)}, 1 \leq j \leq s, 0 \leq i < k_j \quad \text{qui vérifient} \quad (4.4) \text{ et } (4.5). \quad (4.6)$$

Preuve. la preuve est donnée par le théorème 4.4.3 et la discussion ci-dessus. \square

Nous allons maintenant établir une borne supérieure \mathcal{M} sur les tailles binaires des polynômes $Q_i^{(I)}$ des équations (4.5).

Si $H = \mathbb{F}_p$ alors les coefficients des $Q_i^{(I)}$ sont dans \mathbb{F}_p , on prend $\mathcal{M} = \log_2 p$.

Si $H = \mathbb{Q}$, dans ce cas on commence à calculer une borne supérieure sur les longueurs des polynômes $P_i^{(j,I)}$ du théorème 4.3.4 par le lemme suivant :

Lemme 4.4.6 Pour tout $1 \leq j \leq s$, $0 \leq i < k_j$, $|I| \geq 1$ on a :

$$l(P_i^{(j,I)}) \leq sO(nd^3 \log_2(d)) + (2|I| - 1)(\mathcal{D} - 1)(s - 1)$$

Preuve. C'est une conséquence directe du point b) du théorème 4.3.4 et du fait que $M = O(nd^3 \log_2(d))$ est une borne supérieure des tailles binaires des coefficients de g dans H (voir le lemme 4.2.1). \square

Corollaire 4.4.7 Pour tout $2d^3 < |I| \leq 2sd^3$, $0 \leq i \leq \mathcal{D} - 2$ on a :

$$\begin{aligned} l(Q_i^{(I)}) &\leq sO(nd^3 \log_2(d)) + 2(|I| - 1)(\mathcal{D} - 1)(s - 1) \\ &\leq sO(nd^3 \log_2(d)) + 4sd^3(\mathcal{D} - 1)(s - 1). \end{aligned}$$

Preuve. (cas $s = 2$) on a :

$$Q_i^{(I)} = \sum_{1 \leq |J| < |I|, 0 \leq l \leq i} P_l^{(1,J)} P_{i-l}^{(2,I-J)}$$

donc par la proposition 6.1.2 de l'appendice et le lemme 4.4.6, on obtient

$$\begin{aligned} l(Q_i^{(I)}) &\leq \max_{l,J} \left\{ l \left(P_l^{(1,J)} P_{i-l}^{(2,I-J)} \right) \right\} \\ &\leq O(nd^3 \log_2(d)) + 2(|I| - 1)(\mathcal{D} - 1). \square \end{aligned}$$

Corollaire 4.4.8 Le nombre d'équations dans la formule (4.6) est

$$N = (\mathcal{D} - 1) \left(\binom{n + 2sd^3}{n} - \binom{n + 2d^3}{n} \right) + \mathcal{D} \leq d^{O(n)}$$

Le nombre des quantificateurs de cette formule est $\mathcal{D} \leq d$, les degrés de ses équations par rapport aux $\alpha_i^{(j)}$ sont bornés par $D \leq 4d^6$. Leurs degrés par rapport à u sont bornés par $\delta \leq 8d^7$. La taille binaire des coefficients de ses équations dans H est bornée par

$$\mathcal{M} = O(nd^6 \log_2(d))$$

dans le cas où $H = \mathbb{Q}$ ($\mathcal{M} = \log_2 p$ si $H = \mathbb{F}_p$).

Preuve. Le nombre d'équations dans la formule (4.6) est donné par le lemme 6.2.1 de l'appendice. Les autres bornes se déduisent des corollaires 4.4.4 et 4.4.7 en tenant compte que $s \leq \mathcal{D} \leq d$. \square

Lemme 4.4.9 *Soit k une partition de \mathcal{D} , alors on peut produire la décomposition suivante :*

$$U_k = \bigcup_{\beta} \left\{ \bigwedge_{\alpha} (B_{\alpha}^{(\beta)} = 0) \wedge (C^{(\beta)} \neq 0) \right\}$$

avec pour tout α, β on a :

- 1) $B_{\alpha}^{(\beta)}, C^{(\beta)} \in H[u_1, \dots, u_r]$.
- 2) $\deg_u(B_{\alpha}^{(\beta)}), l(B_{\alpha}^{(\beta)}) \leq d^{O(nr d^2)}$.
- 3) $\deg_u(C^{(\beta)}), l(C^{(\beta)}) \leq d^{O(nd)}$.
- 4) Le nombre des α et celui des β sont $\leq d^{O(nr d^2)}$.

Cette décomposition se fait avec

$$d^{O(nr^2 d^3)}$$

opérations dans H . Sa complexité binaire est bornée par

$$p^{O(1)} d^{O(nr^2 d^3)}.$$

Preuve. Par application de l'algorithme d'élimination de quantificateurs de Chistov-Grigoriev [24] (voir aussi le chapitre 2) sur la formule (4.6) qui définit U_k (corollaire 4.4.5) en tenant compte des bornes du corollaire 4.4.8. \square

Les ensembles constructibles U_k où les k sont les partitions de \mathcal{D} ne forment pas une partition de \mathcal{W} parce qu'ils ne sont pas deux à deux disjoints et pour tout $a \in U_k$, la décomposition $g^{(a)} = G_1^{(a)} \cdots G_s^{(a)}$ donnée par le lemme de Hensel n'est pas une factorisation absolue de $g^{(a)}$. Pour avoir une partition de \mathcal{W} en ensembles constructibles et une factorisation absolue de $g^{(a)}$ uniforme sur chacun d'eux, nous introduisons la définition suivante :

Définition 4.4.10 *On dit qu'une partition $k' = (k'_1, \dots, k'_h)$ de \mathcal{D} est plus fine qu'une autre partition $k = (k_1, \dots, k_s)$ de \mathcal{D} si pour tout $1 \leq l \leq s$, $k_l = k'_{i_l} + k'_{i_l+1} \cdots + k'_{i_{l+1}-1}$ pour certains $1 \leq i_1 < \dots < i_s \leq h$.*

Proposition 4.4.11 *Si k' est plus fine que k alors $U_{k'} \subset U_k$.*

Preuve. Voir la définition 4.4.1. \square

Théorème 4.4.12 *Pour chaque couple (\mathcal{W}, g) du lemme 4.2.1, l'ensemble constructible \mathcal{W} se partage sous la forme :*

$$\mathcal{W} = \bigcup_{k \in pt(\mathcal{D})} \mathcal{U}_k$$

où $pt(\mathcal{D})$ est l'ensemble des partitions de \mathcal{D} . Pour chaque \mathcal{U}_k , ils existent de polynômes

$$G_1, \dots, G_s \in H(C_1, \dots, C_{\mathcal{D}}, u)[X, Y_1, \dots, Y_n]$$

où $C_1, \dots, C_{\mathcal{D}}$ sont de nouvelles variables. Pour toute spécialisation des paramètres $a \in \mathcal{U}_k$, il existe $(c_1, \dots, c_{\mathcal{D}}) \in \overline{H}^{\mathcal{D}}$, une solution du système algébrique défini par (4.4) et (4.5) qui vérifient :

- Aucun des dénominateurs des coefficients de G_j ne s'annule en $(c_1, \dots, c_{\mathcal{D}}, a)$.
- $\deg_u(G_j) \leq 8d^6$, $\deg_{C_1, \dots, C_{\mathcal{D}}}(G_j) \leq 4d^5$, $\deg_X(G_j) \leq \mathcal{D} \leq d$, $\deg_Y(G_j) \leq 2d^3$.
- La taille binaire de G_j est $l(G_j) \leq O(nd^5 \log_2(d))$.
- La factorisation absolue du polynôme $g^{(a)} \in \overline{H}[X, Y_1, \dots, Y_n]$ est donnée par :

$$g^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c_1, \dots, c_{\mathcal{D}}, a)}, \quad G_j^{(c_1, \dots, c_{\mathcal{D}}, a)} \text{ est absolument irréductible.}$$

Preuve. Pour tout $k \in pt(\mathcal{D})$ prenons

$$\mathcal{U}_k = U_k \setminus \bigcup_{k' \neq k} U_{k'}$$

la réunion est faite sur les partitions k' de \mathcal{D} plus fine que k . Les ensembles constructibles \mathcal{U}_k , $k \in pt(\mathcal{D})$ forment une partition de \mathcal{W} . Les polynômes G_1, \dots, G_s sont donnés par le lemme de Hensel, leurs coefficients sont de fonctions rationnelles des paramètres u et des coefficients $C_1, \dots, C_{\mathcal{D}}$ de $g_0^{(1)}, \dots, g_0^{(s)}$ (voir théorème 4.3.4). Les bornes sur les degrés et la taille binaire se déduisent du lemme 4.2.1 et du théorème 4.3.4. \square

4.5 Théorème principal

Dans cette section, nous voulons remplacer les variables $C_1, \dots, C_{\mathcal{D}}$ du théorème 4.4.12 par une seule variable C et nous décrivons le passage retour de la factorisation absolue de $g^{(a)}$ donnée par le théorème 4.4.12 à celle de $f^{(a)}$ d'une manière uniforme, ce qui constitue le résultat final de ce chapitre (théorème 4.5.1). L'idée principale de cette section est l'utilisation de l'algorithme de résolution des systèmes algébriques de dimensions zéros du chapitre 3.

Fixons un certain ensemble constructible $\mathcal{U}_k \subset \mathcal{W}$ donné par le théorème 4.4.12 et considérons le système algébrique paramétré S défini par les équations (4.4) et (4.5) ci dessus, les paramètres de ce système sont les variables $u = (u_1, \dots, u_r)$, les inconnues sont les variables $C_1, \dots, C_{\mathcal{D}}$ qui remplacent les $\alpha_i^{(j)}$ dans ces équations. Pour tout $a \in \mathcal{U}_k$ le système $S^{(a)}$ obtenu après spécialisation des paramètres en a dans ses équations admet de solutions (corollaire 4.4.5). En plus, $S^{(a)}$ admet un nombre fini de solutions qui correspondent aux permutations des facteurs de $g_0^{(a)}$ (voir la définition 4.4.1 de U_k).

Les degrés des équations du système S par rapport à u (resp. $C_1, \dots, C_{\mathcal{D}}$) sont bornés par $8d^7$ (resp. $4d^6$), leur nombre est $N \leq d^{O(n)}$. Les tailles binaires des coefficients (dans H) de ces équations sont bornées par $O(nd^6 \log_2(d))$ (voir théorème 4.3.4 et corollaire 4.4.8).

L'algorithme de résolution des systèmes algébriques paramétrés zéro-dimensionnels décrit dans le théorème 3.5.3 du chapitre 3 permet de décomposer \mathcal{U}_k en

$$d^{O(r^2 d^2)}$$

ensembles constructibles \mathcal{V} deux à deux disjoints qui vérifient :

1) Les degrés des équations et des inéquations (dans $H[u]$) qui définissent \mathcal{V} sont bornés par $d^{O(rd^2)}$. Leurs tailles binaires sont $\leq nd^{O(rd^2)}$.

2) Pour chaque \mathcal{V} , l'algorithme calcule de polynômes $\chi, \psi_1, \dots, \psi_{\mathcal{D}} \in H(u)[C]$ où C est une nouvelle variable. Toute spécialisation des paramètres $a \in \mathcal{V}$ vérifie :

- Aucun des dénominateurs des coefficients de $\chi, \psi_1, \dots, \psi_{\mathcal{D}}$ ne s'annule en a .

- Les degrés des coefficients de $\chi, \psi_1, \dots, \psi_{\mathcal{D}}$ par rapport à u sont bornés par $d^{O(rd^2)}$. Leurs tailles binaires sont $\leq nd^{O(rd^2)}$.

- $\deg_C(\chi), \deg_C(\psi_j) \leq d^{O(d)}$ pour tout $1 \leq j \leq \mathcal{D}$.

- Pour toute solution $(c_1, \dots, c_{\mathcal{D}}) \in \overline{H}^{\mathcal{D}}$ du système $S^{(a)}$, il existe $c \in \overline{H}$, racine de $\chi^{(a)} \in \overline{H}[C]$ tel que

$$\begin{cases} c_1 &= \psi_1^{(a)}(c) \\ &\vdots \\ c_{\mathcal{D}} &= \psi_{\mathcal{D}}^{(a)}(c) \end{cases}$$

Nous pouvons maintenant énoncer le théorème principal de ce chapitre :

Théorème 4.5.1 *Sous les notations de la section 1, il existe un algorithme qui partage l'espace des paramètres \mathcal{P} en*

$$d^{O(nr^2 d^2)}$$

ensembles constructibles \mathcal{U} deux à deux disjoints qui vérifient :

1) Chaque \mathcal{U} est donné par des équations et des inéquations dans $H[u]$ de degrés et des tailles binaires bornés par $d^{O(nr d^2)}$.

2) Pour chaque \mathcal{U} l'algorithme calcule de polynômes $f_1, \dots, f_s \in H(C, u)[Z_0, \dots, Z_n]$ ($s \leq d$) et un polynôme $\chi \in H(u)[C]$ où C est une nouvelle variable. Pour toute spécialisation des paramètres $a \in \mathcal{U}$, il existe $c \in \overline{H}$, racine de $\chi^{(a)} \in \overline{H}[C]$ (aucun des dénominateurs des coefficients de χ ne s'annule en a) qui vérifie :

- Aucun des dénominateurs des coefficients de f_m ne s'annule en (c, a) .

- $\deg_C(f_m), \deg_C(\chi) \leq d^{O(d)}, \quad \deg_u(f_m), \deg_u(\chi) \leq d^{O(rd^2)}$.

- Les tailles binaires de f_m et χ sont $\leq nd^{O(rd^2)}$.

- La factorisation absolue du polynôme $f^{(a)} \in \overline{H}[Z_0, \dots, Z_n]$ est donnée par :

$$f^{(a)} = \prod_{1 \leq m \leq s} f_m^{(c,a)}, \quad f_m^{(c,a)} \text{ est absolument irréductible.}$$

En particulier, le nombre des facteurs absolument irréductibles distincts de $f^{(a)}$ est constant sur \mathcal{U} et est égale à s . Par conséquence, si $s = 1$, f est absolument irréductible sur \mathcal{U} .

Cet algorithme se fait avec

$$d^{O(nr^2 d^3)}$$

opérations dans H . Sa complexité binaire est

$$p^{O(1)} d^{O(nr^2 d^3)}$$

Preuve. Reprenons la discussion au dessus du théorème 4.5.1, fixons un ensemble constructible $\mathcal{V} \subset \mathcal{U}_k \subset \mathcal{W}$ où \mathcal{U}_k est donné par le théorème 4.4.12 et (\mathcal{W}, g) est donné par le lemme 4.2.1. Remplaçons les expressions

$$\begin{cases} C_1 &= \psi_1(C) \\ &\vdots \\ C_{\mathcal{D}} &= \psi_{\mathcal{D}}(C) \end{cases}$$

dans les coefficients des polynômes $G_j \in H(C_1, \dots, C_{\mathcal{D}}, u)[X, Y_1, \dots, Y_n]$ du théorème 4.4.12, on obtient de polynômes $g_j \in H(C, u)[X, Y_1, \dots, Y_n]$ qui vérifient :

$$\deg_C(g_j) \leq d^{O(d)} \quad \deg_u(g_j) \leq d^{O(rd^2)}, \quad \deg_X(g_j) \leq d, \quad \deg_Y(g_j) \leq 2d^3.$$

- La taille binaire de g_j est $l(g_j) \leq nd^{O(rd^2)}$.

- Pour tout $a \in \mathcal{V}$, il existe $c \in \overline{H}$, racine de $\chi^{(a)} \in \overline{H}[C]$. La factorisation absolue du polynôme $g^{(a)}$ est donnée par :

$$g^{(a)} = \prod_{1 \leq j \leq s} g_j^{(c,a)}, \quad g_j^{(c,a)} \text{ est absolument irréductible.}$$

Ceci est une factorisation absolue uniforme du polynôme $g \in H(u)[X, Y_1, \dots, Y_n]$ sur \mathcal{V} . Nous allons voir comment obtenir uniformement (i.e., dans le sens du théorème) la factorisation absolue de $f \in H[u][Z_0, \dots, Z_n]$. Pour cela, nous revenons à la forme du polynôme g associé à \mathcal{W} dans la section 2 (revoir la preuve du lemme 4.2.1). Deux formes étaient obtenues :

Cas où $\mathcal{W} = W_{i,t}^{(2,j)}$ pour certain i, t, j fixés :

Dans ce cas $g = g_{i,t,j}$, on calcul la matrice inverse T_i^{-1} de T_i et pour tout $1 \leq m \leq s$ on pose :

$$f_m(Z_0, \dots, Z_n) = g_m(X^{p^t}, Y_1 - c_1^{(j)}, \dots, Y_n - c_n^{(j)}) \in H(C, u)[Z_0, \dots, Z_n]$$

où $(X, Y_1, \dots, Y_n)^{tr} = T_i^{-1}(Z_0, \dots, Z_n)^{tr}$. Ces polynômes vérifient le point 2) du théorème 4.5.1.

Cas où $\mathcal{W} = W_{i,t}^{(1,j)}$ pour certain i, t, j fixés :

Dans ce cas $g = Q_j$, pour tout $a \in \mathcal{V}$, ils existent $c \in \overline{H}$, racine de $\chi^{(a)} \in \overline{H}[C]$ et un vecteur $\alpha = (\alpha_1, \dots, \alpha_s) \in \mathbb{N}^s$ avec $\alpha_1 k_1 + \dots + \alpha_s k_s = \mathcal{D}$ tel que :

$$g_{i,t}^{(a)} = \prod_{1 \leq m \leq s} \left(g_m^{(c,a)} \right)^{\alpha_m}.$$

Cette propriété permet de partager \mathcal{V} en des sous-ensembles constructibles \mathcal{V}_α . Pour tout $1 \leq m \leq s$ posons

$$f_m(Z_0, \dots, Z_n) = g_m^{\alpha_m}(X^{p^t}, Y_1, \dots, Y_n) \in H(C, u)[Z_0, \dots, Z_n]$$

où $(X, Y_1, \dots, Y_n)^{tr} = T_i^{-1}(Z_0, \dots, Z_n)^{tr}$. Ces polynômes vérifient le point 2) du théorème 4.5.1.

Il reste à compter le nombre des ensembles constructibles qui partagent l'espace des paramètres \mathcal{P} et à estimer la complexité totale de l'algorithme. Le lemme 6.3.2 de

l'appendice montre que le nombre des partitions de \mathcal{D} est $\leq \mathcal{D}^{\mathcal{D}+1}$. En tenant compte du nombre des \mathcal{W} (lemme 4.2.1), celui des \mathcal{U}_k ($\leq d^{d+1}$) et celui de \mathcal{V} ($\leq d^{O(r^2 d^2)}$) on obtient le nombre totale des ensembles constructibles du théorème.

Pour tout multi-indice I , le calcul des coefficients de $g_I^{(j)}$, $1 \leq j \leq s$ (i.e., résolution du système linéaire $Bx = b_I$) coûte $O(d^{2.376})$. Pour construire la formule quantifiée (4.6) qui définit U_k , il fallait calculer tous les polynômes $g_I^{(j)}$, $1 \leq j \leq s$, $1 \leq |I| \leq 2sd^3$. La complexité de ce calcul est bornée par

$$\binom{n + 2sd^3}{n} O(d^{2.376}) \leq d^{O(n)}.$$

Puisque le nombre des partitions k de \mathcal{D} est $\leq d^{(d+1)}$ (lemme 6.3.2 de l'appendice), alors la complexité (lemme 4.4.9) de la construction de tous les U_k est

$$d^{d+1} d^{O(nr^2 d^3)} \leq d^{O(nr^2 d^3)}$$

opérations dans H . Sa complexité binaire est $p^{O(1)} d^{O(nr^2 d^3)}$.

La complexité de l'algorithme de résolution des systèmes algébriques paramétrés zéro-dimensionnels (voir le théorème 3.5.3 du chapitre 3) est $d^{O(r^2 d^2)}$ opérations dans H . Sa complexité binaire est $nd^{O(r^2 d^2)}$.

En tenant compte de la complexité du construction des \mathcal{W} (corollaire 4.2.5), on obtient la borne de complexité totale du théorème. \square

4.6 Cas général

Revenons au cas général qui consiste à considérer le corps $F = H(T_1, \dots, T_l)[\eta]$ du chapitre 1. Soit $f \in F[u][Z_0, \dots, Z_n]$ un polynôme paramétré de degré par rapport aux paramètres u borné par δ , son degré par rapport aux variables T_1, \dots, T_l est $\leq d_2$ et sa taille binaire $l(f)$ est $\leq M$. L'espace des paramètres dans ce cas est $\mathcal{P} = \overline{F}^r$.

En suivant les différentes étapes de l'algorithme précédent (théorème 4.5.1) et en tenant compte des bornes établies dans le chapitre 3 sur la résolution de systèmes paramétrés zéro-dimensionnels, on peut produire un algorithme qui partage \mathcal{P} en

$$(\delta dd_1)^{O(nr^2 d^2)}$$

ensembles constructibles \mathcal{U} deux à deux disjoints qui vérifient :

1) Chaque \mathcal{U} est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l sont bornés par $d_2 \delta^{O(r)} (dd_1)^{O(nr d^2)}$. Leurs tailles binaires sont bornées par

$$(M + M_1) l d_2 \delta^{O(r)} (dd_1)^{O(nr d^2)}.$$

2) Pour chaque \mathcal{U} l'algorithme calcule de polynômes $f_1, \dots, f_s \in F(C, u)[Z_0, \dots, Z_n]$ ($s \leq d$) et un polynôme $\chi \in F(u)[C]$ où C est une nouvelle variable. Pour toute spécialisation des paramètres $a \in \mathcal{U}$, il existe $c \in \overline{F}$, racine de $\chi^{(a)} \in \overline{F}[C]$ (aucun des dénominateurs des coefficients de χ ne s'annule en a) qui vérifie :

- Aucun des dénominateurs des coefficients de f_j ($1 \leq j \leq s$) ne s'annule en (c, a) .
- $\deg_C(f_j), \deg_C(\chi) \leq \delta d^{O(d)}, \quad \deg_u(f_j), \deg_u(\chi) \leq \delta^{O(r)} d^{O(rd^2)}.$
- $\deg_{T_1, \dots, T_l}(f_j), \deg_{T_1, \dots, T_l}(\chi) \leq \delta^{O(r)} d_2 d^{O(rd^2)}.$
- Les tailles binaires de f_j et χ sont $\leq n(M + M_1) \delta^{O(r)} d_2 d^{O(rd^2)}.$
- La factorisation absolue du polynôme $f^{(a)} \in \overline{F}[Z_0, \dots, Z_n]$ est donnée par :

$$f^{(a)} = \prod_{1 \leq j \leq s} f_j^{(c, a)}, \quad f_j^{(c, a)} \text{ est absolument irréductible.}$$

La complexité totale de cet algorithme est bornée par

$$(\delta d_2)^{O(r^2 l)} (d d_1)^{O(nr^2 l d^3)}$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(p M M_1)^{O(1)} (\delta d_2)^{O(r^2 l)} (d d_1)^{O(nr^2 l d^3)}.$$

Chapitre 5

Résolution de systèmes algébriques paramétrés de dimensions positives

5.1 Introduction et notations

Considérons un système polynomial paramétré $f_1 = \dots = f_k = 0$ où $f_1, \dots, f_k \in F[u_1, \dots, u_r, X_0, \dots, X_n]$ sont de polynômes paramétrés homogènes en $X = (X_0, \dots, X_n)$ de degrés $\leq d$. Le corps F est le corps utilisé dans les chapitres précédents, i.e., $F := H(T_1, \dots, T_l)[\eta]$ où $H = \mathbb{Q}$ si $\text{car}(F) = 0$ et $H \supset \mathbb{F}_p$ est un corps fini de cardinal supposé (dans ce chapitre) $> kd^n$ si $\text{car}(F) = p > 0$. Les degrés des coefficients de ces polynômes ainsi que leurs tailles binaires sont comme dans le chapitre 3. Ces polynômes sont donnés en représentation dense par leurs vecteurs des coefficients dans H . Les paramètres $u = (u_1, \dots, u_r)$ prennent des valeurs de l'ensemble $\mathcal{P} := \overline{F}^r$ qui est appelé l'espace des paramètres.

On s'intéresse dans ce chapitre à la résolution des systèmes algébriques

$$f_1^{(a)} = \dots = f_k^{(a)} = 0$$

(i.e., la décomposition des variétés projectives $V^{(a)} := V(f_1^{(a)}, \dots, f_k^{(a)}) \subset P^n(\overline{F})$ en composantes absolument irréductibles) d'une manière uniforme sur les valeurs $a \in \mathcal{P}$ des paramètres dans un sens qui sera précisé ci-après (voir corollaire 5.7.1).

Dans la deuxième section, on définit pour chaque $a \in \mathcal{P}$ un arbre $T^{(a)}$ tel que les feuilles de cet arbre sont associées aux composantes absolument irréductibles de la variété $V^{(a)}$. Ces arbres sont appelés les arbres des composantes des systèmes $f_1^{(a)} = \dots = f_k^{(a)} = 0$. Ensuite, on présente le résultat général de ce chapitre (théorème 5.2.5) qui est un algorithme qui calcule toutes les variétés absolument irréductibles associées aux noeuds de l'arbre des composantes. La preuve du théorème 5.2.5, i.e., la construction de ces arbres se fait par un calcul de combinaisons linéaires h_1, \dots, h_{n+1} de f_1, \dots, f_k à coefficients dans le corps H et par un changement paramétrique des variables X_0, \dots, X_n . Ce calcul se fait par induction sur le niveau m des arbres des composantes, la première étape (section 3) n'est autre que l'algorithme de factorisation absolue de polynômes paramétrés présenté au chapitre 4. La formalisation des hypothèses de l'induction se situe dans la section 4. Le coeur de l'induction (i.e., l'étape $m + 1$) constitue le contenu du section 5.

5.2 Arbres des composantes

A chaque spécialisation $a \in \mathcal{P}$ des paramètres, on définit un arbre $T^{(a)}$ des composantes associé au système $f_1^{(a)} = \dots = f_k^{(a)} = 0$ de la façon suivante (voir [58] dans le cas non paramétrique) :

La racine de $T^{(a)}$ est l'espace projectif $P^n(\overline{F})$ tout entier, le niveau d'un certain noeud de cet arbre est le nombre des branches qui le relient au racine. Le nombre des niveaux de l'arbre $T^{(a)}$ est au plus $n + 1$. Pour chaque noeud de niveau m (noté v_m), on associe une variété projective $W_{v_m}^{(a)} \subset P^n(\overline{F})$, absolument irréductible de codimension m

(pour $m = n + 1$, on prend $W_{v_{n+1}}^{(a)} = \emptyset$). La construction de ces variétés est basée sur le lemme suivant :

Lemme 5.2.1 *Il existe un algorithme qui partage l'espace des paramètres \mathcal{P} en un nombre fini d'ensembles constructibles. Pour chaque ensemble \mathcal{U} parmi eux, l'algorithme calcule des combinaisons linéaires h_1, \dots, h_{n+1} de f_1, \dots, f_k à coefficients dans le corps H tel que tout $a \in \mathcal{U}$ vérifie la propriété suivante :*

Pour tout $1 \leq m \leq n + 1$, la codimension de chaque composante absolument irréductible de la variété $V(h_1^{(a)}, \dots, h_m^{(a)}) \subset P^n(\overline{F})$ qui n'est pas une composante absolument irréductible de $V^{(a)}$ est m . Par conséquent $V^{(a)} = V(h_1^{(a)}, \dots, h_{n+1}^{(a)})$.

Supposons pour le moment que ce lemme est démontré et fixons un ensemble constructible \mathcal{U} de cette partition de \mathcal{P} avec les polynômes h_1, \dots, h_{n+1} associés. Retournons à la construction des arbres $T^{(a)}$ pour $a \in \mathcal{U}$, les fils de la racine sont les composantes absolument irréductibles de l'hypersurface $V(h_1^{(a)})$. Pour un noeud v_m de l'arbre, ses fils sont les composantes absolument irréductibles de la variété

$$\mathcal{W}_{v_m}^{(a)} := W_{v_m}^{(a)} \cap V(h_{m+1}^{(a)}).$$

On peut distinguer deux catégories des noeuds :

Définition 5.2.2 *Un noeud v_m de l'arbre $T^{(a)}$ est dit du premier type (i.e., v_m est une feuille de $T^{(a)}$) si la variété $W_{v_m}^{(a)}$ est une composante absolument irréductible de $V^{(a)}$ et v_m est dit du second type si $W_{v_m}^{(a)} \not\subseteq V^{(a)}$.*

Corollaire 5.2.3 *Pour tout $1 \leq m \leq n + 1$, les composantes absolument irréductibles de la variété $V(h_1^{(a)}, \dots, h_m^{(a)})$ sont les variétés $W_{v_m}^{(a)}$ pour tous les noeuds v_m de niveau m de $T^{(a)}$ et les variétés $W_{v_j}^{(a)}$ ($j < m$) qui sont des composantes de $V^{(a)}$ (i.e., les feuilles v_j de l'arbre de niveaux $j < m$).*

Preuve. La démonstration se fait par induction sur m en se basant sur la construction ci-dessus des arbres des composantes. \square

Proposition 5.2.4 *Pour tout $a \in \mathcal{U}$, toutes les composantes absolument irréductibles de $V^{(a)}$ sont à l'intérieur de $T^{(a)}$, i.e, pour une composante W de $V^{(a)}$, de codimension m , il existe une feuille v_m de $T^{(a)}$ de niveau m tel que $W = W_{v_m}^{(a)}$.*

Preuve. On a $W \subset V^{(a)} \subset V(h_1^{(a)}, \dots, h_m^{(a)})$, alors W est contenue dans une composante absolument irréductible de $V(h_1^{(a)}, \dots, h_m^{(a)})$, mais $W \not\subseteq W_{v_j}^{(a)}$ pour toute feuille v_j de niveau $j < m$, alors il existe un noeud v_m de $T^{(a)}$ tel que $W \subset W_{v_m}^{(a)}$ (corollaire 5.2.3), or $\dim W = \dim W_{v_m}^{(a)} = n - m$ donc $W = W_{v_m}^{(a)}$. \square

Dans la suite de ce chapitre, on démontre un résultat plus important que le lemme 5.2.1, celui-ci donne une partition plus fine de l'espace des paramètres en ensembles constructibles et calcule toutes les variétés $W_{v_m}^{(a)}$ pour tout noeud v_m de l'arbre $T^{(a)}$ d'une manière uniforme sur chaque élément de cette partition :

Théorème 5.2.5 *Sous les notations et les hypothèses ci-dessus, il existe un algorithme qui partage l'espace des paramètres \mathcal{P} en*

$$k(\delta dd_1)^{r^3 d^{O(n^3)}}$$

ensembles constructibles \mathcal{U} tels que tout ensemble \mathcal{U} vérifie les propriétés suivantes :

1) \mathcal{U} est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l bornés par

$$d_2 \delta^{O(r^3)} (dd_1)^{r^3 d^{O(n^3)}}.$$

Leurs tailles binaires sont bornées par $(M_1 + M_2) d_2 \delta^{O(r^3)} (dd_1)^{r^3 d^{O(n^3)}}$.

2) *Pour tout $1 \leq m \leq n + 1$, le nombre des noeuds de niveau m est constant sur \mathcal{U} , i.e., pour tout $a, b \in \mathcal{U}$, le nombre des noeuds v_m de l'arbre $T^{(a)}$ est égale à celui de $T^{(b)}$.*

3) *L'algorithme calcule une base Y_0, \dots, Y_n de l'espace des formes linéaires en X_0, \dots, X_n à coefficients dans H . Chaque variété absolument irréductible W_{v_m} de codimension m , est donnée par **un système représentatif paramétrique et un point générique efficace paramétrique** au sens suivant :*

Système représentatif paramétrique :

Pour chaque \mathcal{U} , l'algorithme calcule des polynômes $\psi_1, \dots, \psi_N \in F(C, u_1, \dots, u_r)[Y_0, \dots, Y_n]$ homogènes en Y_0, \dots, Y_n de degré $\leq d^{O(m)}$ et un polynôme $\chi \in F(u_1, \dots, u_r)[C]$. Pour tout $a \in \mathcal{U}$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ (les coefficients de χ sont bien définis sur \mathcal{U}) qui vérifient :

- *Aucun des dénominateurs des coefficients de ψ_1, \dots, ψ_N ne s'annule en (c, a) .*
- $\deg_C(\psi_j) \leq \delta d^{O(n^3 d)}, \quad \deg_C(\chi) \leq \delta^{O(r^2)} d^{r^2 d^{O(n^3)}}.$
- $\deg_u(\psi_j) \leq \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_u(\chi) \leq \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}.$
- $\deg_{T_1, \dots, T_l}(\psi_j) \leq d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_{T_1, \dots, T_l}(\chi) \leq d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}.$
- *Les tailles binaires des coefficients de ψ_j (resp. χ) sont bornées par $(M_1 + M_2) d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$ (resp. $(M_1 + M_2) d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$).*
- $N \leq d^{O(n^2)}.$

- Les polynômes homogènes $\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)} \in \overline{F}[Y_0, \dots, Y_n]$ définissent la variété $W_{v_m}^{(a)}$, i.e.,

$$W_{v_m}^{(a)} = V(\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)}) \subset P^n(\overline{F}).$$

Point générique efficace paramétrique :

i) La variété $W_{v_m}^{(a)}$ n'est pas contenue dans l'hyperplan $V(Y_0) \subset P^n(\overline{F})$.

ii) Les fonctions rationnelles $t_1 = \frac{Y_1}{Y_0}, \dots, t_{n-m} = \frac{Y_{n-m}}{Y_0}$ sur $W_{v_m}^{(a)}$ forment une base de transcendance de $\overline{F}(W_{v_m}^{(a)})$ sur \overline{F} .

iii) Pour chaque \mathcal{U} , l'algorithme calcule des polynômes $\phi, B_1, \dots, B_n \in F(C, u_1, \dots, u_r)(t_1, \dots, t_{n-m})[Z]$ et une fonction rationnelle $\theta = \sum_{0 \leq j \leq n} \alpha_j \frac{Y_j}{Y_0}$ avec $0 \leq \alpha_j \leq \deg(W_{v_m}^{(a)}) \leq d^m$. Il calcule aussi une puissance p^ν ($p^\nu = 1$ si $\text{car}(F) = 0$ et $\nu \geq 0$ si $\text{car}(F) = p > 0$). Pour tout $a \in \mathcal{U}$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ vérifiant :

- Aucun des dénominateurs des coefficients de ϕ, B_1, \dots, B_n dans $F(C, u_1, \dots, u_r)$ ne s'annule en (c, a) .

- $\deg_C(B_j) \leq \delta d^{O(n^3 d)}, \quad \deg_C(\phi) \leq \delta^{O(r^2)} d^{r^2 d^{O(n^3)}}.$

- $\deg_u(B_j) \leq \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_u(\phi) \leq \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}.$

- $\deg_{t_1, \dots, t_{n-m}}(B_j), \deg_{t_1, \dots, t_{n-m}}(\phi) \leq d^{O(n^3)}.$

- $\deg_{T_1, \dots, T_l}(B_j) \leq d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_{T_1, \dots, T_l}(\phi) \leq d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}.$

- $\deg_Z(B_j) < \deg_Z(\phi) \leq d^{O(m)}$ et $p^\nu \leq d^{O(m)}.$

- Les tailles binaires des coefficients de B_j (resp. ϕ) sont bornées par $(M_1 + M_2)d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$ (resp. $(M_1 + M_2)d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}).$

- Un point générique efficace de la variété $W_{v_m}^{(a)}$ est donné par l'isomorphisme de corps suivant :

$$\tau : \overline{F}\left(1, \left(\frac{Y_1}{Y_0}\right)^{p^\nu}, \dots, \left(\frac{Y_n}{Y_0}\right)^{p^\nu}\right) \longrightarrow \overline{F}(t_1, \dots, t_{n-m})[\theta] \quad (5.1)$$

Cet isomorphisme est défini par la représentation univariée polynomiale suivante des

éléments de $W_{v_m}^{(a)}$:

$$\phi^{(c,a)}(t_1, \dots, t_{n-m}, \theta) = 0, \begin{cases} \left(\frac{Y_1}{Y_0}\right)^{p^\nu} &= B_1^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \\ \vdots & \\ \left(\frac{Y_n}{Y_0}\right)^{p^\nu} &= B_n^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \end{cases}$$

où θ est algébrique sur le corps $\overline{F}(t_1, \dots, t_{n-m})$, racine du polynôme $\phi^{(c,a)} \in \overline{F}(t_1, \dots, t_{n-m})[Z]$. Ceci définit un point générique efficace des variétés $W_{v_m}^{(a)}$ d'une manière uniforme sur chaque \mathcal{U} .

La démonstration de ce théorème se fait par induction sur le niveau m des arbres des composantes (i.e., la codimension). Dans chaque étape de cette induction, l'espace des paramètres \mathcal{P} sera partagé convenablement pour aboutir aux résultats souhaités dans le théorème 5.2.5 :

5.3 Base de l'induction

Pour $m = 1$, on prend $h_1 = f_1 \in F[u_1, \dots, u_r, X_0, X_1, \dots, X_n]$, l'algorithme de factorisation absolue de polynômes paramétrés décrit au chapitre 4 partage l'espace des paramètres en (au plus)

$$(\delta dd_1)^{O(nr^2d^2)}$$

ensembles constructibles U_1 deux à deux disjoints qui vérifient :

1) Chaque ensemble U_1 est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l sont bornés par $d_2\delta^{O(r)}(dd_1)^{O(nrd^2)}$. Leurs tailles binaires sont bornées par

$$(M_1 + M_2)ld_2\delta^{O(r)}(dd_1)^{O(nrd^2)}.$$

2) Pour chaque U_1 , l'algorithme calcule des polynômes $G_1, \dots, G_s \in F(C, u)[X_0, \dots, X_n]$ ($s \leq d$) et un polynôme $\chi \in F(u)[C]$ où C est une nouvelle variable. Pour toute spécialisation des paramètres $a \in U_1$, il existe $c \in \overline{F}$, racine de $\chi^{(a)} \in \overline{F}[C]$ (aucun des dénominateurs des coefficients de χ ne s'annule en a) qui vérifie :

- Aucun des dénominateurs des coefficients de G_j ne s'annule en (c, a) .

- $\deg_C(G_j), \deg_C(\chi) \leq \delta d^{O(d)}, \deg_u(G_j), \deg_u(\chi) \leq \delta^{O(r)}d^{O(rd^2)}$.

- $\deg_{T_1, \dots, T_l}(G_j), \deg_{T_1, \dots, T_l}(\chi) \leq \delta^{O(r)}d_2d^{O(rd^2)}$.

- Les tailles binaires de G_j et χ sont $\leq n(M_1 + M_2)\delta^{O(r)}d_2d^{O(rd^2)}$.

- Chaque G_j est homogène en X_0, \dots, X_n de degré inférieur ou égale à d .
- La factorisation absolue du polynôme $h_1^{(a)} \in \overline{F}[X_0, \dots, X_n]$ est donnée par :

$$h_1^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c,a)}, \quad G_j^{(c,a)} \text{ est absolument irréductible.}$$

La famille des variétés $W_{v_1}^{(a)}$ où v_1 est un noeud de niveau 1, coïncide avec la famille des composantes absolument irréductibles de la variété $V(h_1^{(a)}) \subset P^n(\overline{F})$, cette dernière famille est formée par les hypersurfaces $W_j^{(a)} := V(G_j^{(c,a)})$. Chaque $W_j^{(a)}$ est définie paramétriquement par le polynôme homogène G_j , i.e., $\{G_j\}$ est un système représentatif paramétrique de la variété $W_j^{(a)}$ au sens du théorème 5.2.5.

Pour construire paramétriquement un point générique *efficace* de chaque $W_j^{(a)}$, il faut tout d'abord calculer une base de transcendance de l'extension $\overline{F}(W_j^{(a)})$ sur \overline{F} . Pour cela, nous utilisons le lemme 2.2 de [58] avec son corollaire qui calcule une base de transcendance de chaque composante de dimension maximale d'une variété projective donnée (i.e., une composante de dimension égale à celle de la variété) :

Lemme 5.3.1 *Soit $V = V(g_1, \dots, g_s) \subset P^n(\overline{F})$ une variété projective de codimension m , définie par de polynômes homogènes $g_1, \dots, g_s \in F[X_0, \dots, X_n]$. Alors les conditions suivantes sont équivalentes :*

1) $V \cap V(X_0, \dots, X_{n-m}) = \emptyset$

2) le système d'équations

$$g_i(X_0, t_1 X_0, \dots, t_{n-m} X_0, X_{n-m+1}, \dots, X_n) = 0, \quad 1 \leq i \leq s$$

à coefficients dans le corps $F(t_1, \dots, t_{n-m})$ où t_1, \dots, t_{n-m} sont algébriquement indépendants sur F , a un nombre fini de solutions dans $P^m(\overline{F}(t_1, \dots, t_{n-m}))$ et n'admet pas de solutions à l'infini (i.e., solutions qui sont contenues dans l'hyperplan $V(X_0)$).

De plus, si ces conditions sont vérifiées et si W est une composante irréductible de V de dimension maximale (i.e., $\dim(W) = n - m$) alors les fonctions rationnelles $\frac{X_1}{X_0}, \dots, \frac{X_{n-m}}{X_0}$ forment une base de transcendance de $\overline{F}(W)$ sur \overline{F} .

Preuve.

1) \implies 2) : L'ensemble des solutions du système du point 2) est en bijection avec l'ensemble $V_1 \subset P^n(\overline{F}(t_1, \dots, t_{n-m}))$ des solutions du système

$$g_1 = \dots = g_s = 0, \quad X_1 - t_1 X_0 = \dots = X_{n-m} - t_{n-m} X_0 = 0.$$

D'une part $V_1 \cap V(X_0) = V \cap V(X_0, \dots, X_{n-m}) = \emptyset$, d'autre part par le théorème de la dimension de l'intersection [125, 112, 101, 31] on a $\dim(V_1 \cap V(X_0)) \geq \dim(V_1) - 1$ donc $\dim(V_1) \leq 0$ et par suite V_1 est un ensemble fini. Si $V_1 \cap V(X_0) \neq \emptyset$ alors $V \cap V(X_0, \dots, X_{n-m}) \neq \emptyset$, ceci est en contradiction avec la condition 1).

2) \implies 1) : Supposons qu'il existe un élément $(0 : \dots : 0 : \xi_{n-m+1} : \dots : \xi_n) \in V \cap V(X_0, \dots, X_{n-m})$. Alors $(0 : \xi_{n-m+1} : \dots : \xi_n) \in P^m(\overline{F(t_1, \dots, t_{n-m})})$ est une solution à l'infini de 2).

Soit W une composante irréductible de V de dimension maximale. Supposons que X_0 s'annule identiquement sur W alors $W \cap V(X_1, \dots, X_{n-m}) = W \cap V(X_0, \dots, X_{n-m}) \subset V \cap V(X_0, \dots, X_{n-m}) = \emptyset$, d'où la contradiction par le théorème de la dimension de l'intersection qui montre que $\dim(W \cap V(X_1, \dots, X_{n-m})) \geq \dim W - (n - m) = 0$. Donc les fonctions rationnelles $\frac{X_1}{X_0}, \dots, \frac{X_{n-m}}{X_0}$ sont bien définies sur W .

Il reste à prouver que ces fonctions rationnelles sont algébriquement indépendantes sur F . Supposons qu'il existe un polynôme multivarié homogène $\psi \in F[X_0, \dots, X_{n-m}]$ tel que $\psi(X_0, \dots, X_{n-m}) = 0$ sur W . Par une transformation linéaire on peut supposer que $lc_{X_0}(\psi) = 1$, alors d'une part $W \cap V(X_1, \dots, X_{n-m}) = W \cap V(X_1, \dots, X_{n-m}) \cap V(\psi(X_0, \dots, X_{n-m})) = W \cap V(X_0, \dots, X_{n-m}) = \emptyset$, d'autre part par le théorème de la dimension de l'intersection on a $\dim(W \cap V(X_1, \dots, X_{n-m})) \geq 0$, ceci conduit à une contradiction, ce qui prouve le lemme. \square

En général, $W_j^{(a)} \cap V(X_0, \dots, X_{n-1}) \neq \emptyset$, on ne peut pas donc appliquer directement le lemme 5.3.1 sur la variété $W_j^{(a)}$. Par contre le lemme suivant [58] montre l'existence de formes linéaires Y_0, \dots, Y_{n-1} en X_0, \dots, X_n à coefficients dans le corps H qui vérifient :

$$W_j^{(a)} \cap V(Y_0, \dots, Y_{n-1}) = \emptyset.$$

Lemme 5.3.2 *On peut construire une famille $M_{n,n-m,d}$ formé des $(n - m + 1)$ -uplets des formes linéaires en X_0, \dots, X_n à coefficients dans H tel que pour toute variété $V \subset P^n(\overline{F})$, $\text{codim}(V) = m$, $\deg(V) \leq d$, il existe $(Y_0, \dots, Y_{n-m}) \in M_{n,n-m,d}$ avec*

$$V \cap V(Y_0, \dots, Y_{n-m}) = \emptyset.$$

En plus, $\text{card}(M_{n,n-m,d}) = \binom{nd+1}{n-m+1}$ et $M_{n,n-m,d}$ est construit dans un temps polynomial en $\text{card}(M_{n,n-m,d})$.

Preuve. Soit $N = 1 + nd$ et $\alpha_1, \dots, \alpha_N \in H$ distincts deux à deux, considérons les formes linéaires $Y_i = \sum_{0 \leq j \leq n} \alpha_i^j X_j$ pour tout $1 \leq i \leq N$. Montrons que l'ensemble des collections $(Y_{i_0}, \dots, Y_{i_{n-m}})$ où $1 \leq i_0 < \dots < i_{n-m} \leq N$ vérifie les conditions du lemme.

En effet, soit V une variété projective de codimension m , de degré $\leq d$, montrons par induction que pour tout $0 \leq l \leq n - m$, il existe $1 \leq i_0 < \dots < i_l \leq N$ tel

que $\dim(V \cap V(Y_{i_0}, \dots, Y_{i_l})) = n - m - l - 1$. En particulier, pour $l = n - m$ on a $V \cap V(Y_{i_0}, \dots, Y_{i_{n-m}}) = \emptyset$. Supposons que cette propriété est vraie jusqu'à $l - 1$, il suffit de prouver qu'il existe une forme linéaire Y_j , $1 \leq j \leq N$ qui ne s'annule pas identiquement sur la variété $V_1 = V \cap V(Y_{i_0}, \dots, Y_{i_{l-1}})$. Sinon, puisque $\deg(V_1) \leq \deg V \leq d$ alors par le principe de Dirichlet (voir l'appendice), il existe une composante V_2 de V_1 et $(n + 1)$ formes linéaires Y_{j_0}, \dots, Y_{j_n} qui s'annulent identiquement sur V_2 et donc $V_2 \subset V(Y_{j_0}, \dots, Y_{j_n}) = \emptyset$ car la matrice du système linéaire homogène qui définit la variété $V(Y_{j_0}, \dots, Y_{j_n})$ est la matrice de Vandermonde. D'où la contradiction, ce qui prouve le lemme. \square

Dans [48], on trouve une version affine et zéro-dimensionnelle du lemme 5.3.2 :

Lemme 5.3.3 *Soit Γ un sous-ensemble fini de c éléments de H et d un entier vérifiant $(n - 1)d < c$. Pour tout sous-ensemble fini V de \overline{F}^n , de cardinal au plus d , il existe $\alpha \in \Gamma$ tel que $V \cap V(Y) = \emptyset$ où $Y = X_1 + \alpha X_2 + \dots + \alpha^{n-1} X_n$.*

Preuve. Soit Z une nouvelle variable et $P(Z)$ un polynôme défini par

$$P(Z) := \prod_{(\xi_1, \dots, \xi_n) \in V} (\xi_1 + \xi_2 Z + \dots + \xi_n Z^{n-1}).$$

Ce polynôme est non-nul et de degré borné par $(n - 1)d$. Puisque $\text{card}(\Gamma) > (n - 1)d$, il existe $\alpha \in \Gamma$ tel que $P(\alpha) \neq 0$. Ce qui prouve le lemme. \square

Remarque 5.3.4 *Une meilleure construction des lemmes 5.3.2 et 5.3.3 se trouve dans [26], mais dans notre cas, celle-ci n'améliore pas les bornes sur les degrés de la sortie de notre algorithme.*

Pour tout $a \in U_1$, $\dim(W_j^{(a)}) = n - 1$ et $\deg(W_j^{(a)}) \leq d$, le lemme 5.3.2 assure l'existence d'un élément $(Y_0, \dots, Y_{n-1}) \in M_{n,n-1,d}$ tel que $W_j^{(a)} \cap V(Y_0, \dots, Y_{n-1}) = \emptyset$. Ceci permet de décomposer chaque ensemble U_1 en des ensembles constructibles $\tilde{U}_{1,t}$, $1 \leq t \leq \text{card}(M_{n,n-1,d})$ définis par :

$$\tilde{U}_{1,t} = U_{1,t} \setminus \bigcup_{1 \leq t' < t} U_{1,t'}$$

où

$$U_{1,t} = \{a \in U_1, \quad W_j^{(a)} \cap V(Y_0^{(t)}, \dots, Y_{n-1}^{(t)}) = \emptyset \quad \text{pour tout } 1 \leq j \leq s\}.$$

Fixons un certain t et posons $Y_0^{(t)} = Y_0, \dots, Y_{n-1}^{(t)} = Y_{n-1}$ qui sont linéairement indépendantes sur H par construction (voir la preuve du lemme 5.3.2), complétons-les en une base Y_0, \dots, Y_n de l'espace des formes linéaires en X_0, \dots, X_n à coefficients dans H . En exprimant X_0, \dots, X_n en fonction de cette base, on peut représenter chaque G_j comme un élément de $F(C, u_1, \dots, u_r)[Y_0, \dots, Y_n]$. Pour tout $a \in \tilde{U}_{1,t}$, il existe $c \in \overline{F}$, racine de $\chi^{(a)}$ avec $W_j^{(a)} \cap V(Y_0, \dots, Y_{n-1}) = \emptyset$ pour tout $1 \leq j \leq s$. Le lemme 5.3.1 montre donc que les fonctions rationnelles $t_1 = \frac{Y_1}{Y_0}, \dots, t_{n-1} = \frac{Y_{n-1}}{Y_0}$ forment une base de transcendance de $\overline{F}(W_j^{(a)})$ sur \overline{F} pour tout j .

Proposition 5.3.5 *Chaque $U_{1,t}$ est un sous-ensemble constructible de U_1 . Les degrés des équations et des inéquations qui le définissent par rapport à u (resp. T_1, \dots, T_l) sont bornés par*

$$\delta^{O(r)} d^{O(rd^2)}$$

(resp. $\delta^{O(r)} d_1^{O(1)} d_2^{O(rd^2)}$). Leurs tailles binaires sont bornées par

$$n(M_1 + M_2) \delta^{O(r)} d_1^{O(1)} d_2^{O(rd^2)}$$

Preuve. $a \in U_{1,t}$ si et seulement si $(0 : \dots : 0 : 1) \notin W_j^{(a)} \subset P^n(\overline{F})$ pour tout $1 \leq j \leq s$. Alors $U_{1,t}$ est la \overline{F} -réalisation dans U_1 de la formule quantifiée suivante :

$$\exists C, \quad G_j(0, \dots, 0, 1) \neq 0, \chi(C) = 0 \quad 1 \leq j \leq s.$$

Les degrés des atomes de cette formule par rapport à C (resp. u et T_1, \dots, T_l) sont

$$\leq \delta d^{O(d)}$$

(resp. $\leq \delta d^{O(rd^2)}$ et $\leq \delta d_2 d^{O(rd^2)}$), leur nombre est au plus $d + 1$. Par application de l'algorithme d'élimination de quantificateurs décrit dans [24] (voir aussi le chapitre 2) sur cette formule, on obtient les bornes sur les degrés des équations et des inéquations qui définissent $U_{1,t}$. \square

Fixons aussi j et posons $G_j = \tilde{G}_j(Y_0^{p^{\nu_j}}, \dots, Y_n^{p^{\nu_j}})$ avec $\tilde{G}_j \in F(C, u_1, \dots, u_r)[Z_0, \dots, Z_n]$ (Z_0, \dots, Z_n sont de nouvelles variables) et ν_j est le plus grand entier possible ($p^{\nu_j} = 1$ si $\text{car}(F) = 0$), alors pour tout $a \in \tilde{U}_{1,t}$,

$$G_j^{(c,a)} = \tilde{G}_j^{(c,a)}(Y_0^{p^{\nu_j}}, \dots, Y_n^{p^{\nu_j}}) \text{ et } \tilde{G}_j^{(c,a)} \text{ est absolument irréductible.}$$

Posons $\theta_j = \left(\frac{Y_n}{Y_0}\right)^{p^{\nu_j}}$ et

$$\phi_j(Z) = \tilde{G}_j(1, t_1, \dots, t_{n-1}, Z) \in F(C, u_1, \dots, u_r)(t_1, \dots, t_{n-1})[Z]$$

Pour tout $a \in \tilde{U}_{1,t}$, le polynôme $\phi_j^{(c,a)}(Z) \in \overline{F}(t_1, \dots, t_{n-1})[Z]$ admet θ_j comme racine (par le lemme 2.2.8 du chapitre 2) et vérifie :

$$\deg_C(\phi_j) \leq \delta d^{O(d)}, \quad \deg_u(\phi_j) \leq \delta^{O(r)} d^{O(rd^2)}, \quad \deg_{T_1, \dots, T_l}(\phi_j) \leq \delta^{O(r)} d_2 d^{O(rd^2)}$$

$$\deg_{t_1, \dots, t_{n-1}}(\phi_j) \leq d \text{ et } \deg_Z(\phi_j) \leq d.$$

Un point générique *efficace* de $W_j^{(a)}$ est donc donné par l'isomorphisme de corps suivant :

$$\tau_1 : \overline{F}(t_1, \dots, t_{n-1})[\theta_j] \longrightarrow \overline{F}\left(\frac{Y_1}{Y_0}, \dots, \frac{Y_{n-1}}{Y_0}, \left(\frac{Y_n}{Y_0}\right)^{p^{\nu_j}}\right)$$

défini par $\tau_1(t_l) = \frac{Y_l}{Y_0}$, $1 \leq l \leq n-1$, $\tau_1(\theta_j) = \left(\frac{Y_n}{Y_0}\right)^{p^{\nu_j}}$.

Ceci termine la construction des toutes les variétés absolument irréductibles $W_{v_1}^{(a)}$ (les v_1 sont les noeuds de $T^{(a)}$ de niveau 1) par des systèmes représentatifs paramétriques et par des points génériques efficaces paramétriques. Le lemme suivant établie une borne supérieure sur la complexité de cette première étape.

Lemme 5.3.6 *La base de l'induction se fait avec*

$$(\delta d_2)^{O(r^2 l)} (dd_1)^{O(nr^2 l d^3)}$$

opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (dd_1)^{O(nr^2 l d^3)}.$$

Preuve. La complexité de l'algorithme de factorisation absolue de polynômes paramétrés appliqué sur le polynôme h_1 est

$$(\delta d_2)^{O(r^2 l)} (dd_1)^{O(nr^2 l d^3)}$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (dd_1)^{O(nr^2 l d^3)}.$$

Pour tout $1 \leq t \leq \text{card}(M_{n,n-1,d}) \leq \binom{nd+1}{n} \leq d^{O(n)}$, la construction de $U_{1,t}$ se fait par application de l'algorithme d'élimination de quantificateurs sur la formule du preuve de la proposition 5.3.5 en utilisant

$$\delta^{O(r^2 l)} (d_1 d_2)^{O(r l)} d^{O(r^2 l d^2)}$$

opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} \delta^{O(r^2 l)} (d_1 d_2)^{O(r l)} d^{O(r^2 l d^2)}. \square$$

5.4 Hypothèses de l'induction

On suppose qu'à l'étape $m+1$ de l'induction, les polynômes h_1, \dots, h_m sont construits, l'espace des paramètres est partagé en

$$\mathcal{N}_m \leq (\delta d d_1)^{O(m n r^2 d^2)}$$

ensembles constructibles U_m deux à deux disjoints vérifiant :

1) Chaque U_m est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l bornés par

$$d_2 \delta^{O(r)} (dd_1)^{O(mnrd^2)}$$

Leurs tailles binaires sont bornées par

$$(M_1 + M_2) l d_2 \delta^{O(r)} (dd_1)^{O(mnrd^2)}$$

2) Pour chaque U_m , il existe une base Y_0, \dots, Y_n de l'espace des formes linéaires en X_0, \dots, X_n à coefficients dans H . Chaque variété absolument irréductible W_{v_j} de codimension $j \leq m$, associée au noeud v_j , est donnée par **un système représentatif paramétrique** et **un point générique efficace paramétrique** au sens du théorème 5.2.5, i.e., par exemple, pour une variété W_{v_m} :

Système représentatif paramétrique :

Pour chaque U_m , on suppose qu'ils existent des polynômes $\psi_1, \dots, \psi_N \in F(C, u_1, \dots, u_r)[Y_0, \dots, Y_n]$ homogènes en Y_0, \dots, Y_n de degrés $\leq d^{O(m)}$ et un polynôme $\chi \in F(u_1, \dots, u_r)[C]$. Pour tout $a \in U_m$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ (les coefficients de χ sont bien définis sur U_m) qui vérifient :

- Aucun des dénominateurs des coefficients de ψ_1, \dots, ψ_N ne s'annule en (c, a) .
- $\deg_C(\psi_j), \deg_C(\chi) \leq \delta d^{O(md)}$.
- $\deg_u(\psi_j), \deg_u(\chi) \leq \delta^{O(r)} d^{O(mrd^2)}$.
- $\deg_{T_1, \dots, T_l}(\psi_j), \deg_{T_1, \dots, T_l}(\chi) \leq \delta^{O(r)} d_2 d^{O(mrd^2)}$.
- Les tailles binaires des coefficients de ψ_j et χ sont bornées par $(M_1 + M_2) \delta^{O(r)} d_2 d^{O(mrd^2)}$.
- $N \leq d^{O(mn)}$.
- Les polynômes homogènes $\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)} \in \overline{F}[Y_0, \dots, Y_n]$ définissent la variété $W_{v_m}^{(a)}$, i.e.,

$$W_{v_m}^{(a)} = V(\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)}) \subset P^n(\overline{F}).$$

Point générique efficace paramétrique :

- i) La variété $W_{v_m}^{(a)}$ n'est pas contenue dans l'hyperplan $V(Y_0) \subset P^n(\overline{F})$.
- ii) Les fonctions rationnelles $t_1 = \frac{Y_1}{Y_0}, \dots, t_{n-m} = \frac{Y_{n-m}}{Y_0}$ sur $W_{v_m}^{(a)}$ forment une base de transcendance de $\overline{F}(W_{v_m}^{(a)})$ sur \overline{F} .
- iii) Pour chaque U_m , on suppose qu'ils existent des polynômes $\phi, B_1, \dots, B_n \in F(C, u_1, \dots, u_r)(t_1, \dots, t_{n-m})[Z]$, une fonction rationnelle $\theta = \sum_{0 \leq j \leq n} \alpha_j \frac{Y_j}{Y_0}$ et une puissance p^ν ($p^\nu = 1$ si $\text{car}(F) = 0$ et $\nu \geq 0$ si $\text{car}(F) = p > 0$). Pour tout $a \in U_m$, il existe $c \in \overline{F}$ racine de $\chi^{(a)} \in \overline{F}[C]$ vérifiant :
- Aucun des dénominateurs des coefficients de ϕ, B_1, \dots, B_n dans $F(C, u_1, \dots, u_r)$ ne s'annule en (c, a) .
 - $\deg_C(B_j), \deg_C(\phi) \leq \delta d^{O(md)}, \quad \deg_u(B_j), \deg_u(\phi) \leq \delta^{O(r)} d^{O(mrd^2)}$.
 - $\deg_{t_1, \dots, t_{n-m}}(B_j), \deg_{t_1, \dots, t_{n-m}}(\phi) \leq d^{O(m)}$.
 - $\deg_{T_1, \dots, T_l}(B_j), \deg_{T_1, \dots, T_l}(\phi) \leq d_2 \delta^{O(r)} d^{O(mrd^2)}$.
 - $\deg_Z(B_j) < \deg_Z(\phi) \leq d^{O(m)}$ et $p^\nu \leq d^{O(m)}$.
 - Les tailles binaires des coefficients de B_j et ϕ sont bornées par $(M_1 + M_2) d_2 \delta^{O(r)} d^{O(mrd^2)}$.
 - Un point générique *efficace* de la variété $W_{v_m}^{(a)}$ est défini par les expressions suivantes :

$$\phi^{(c,a)}(t_1, \dots, t_{n-m}, \theta) = 0, \quad \begin{cases} \left(\frac{Y_1}{Y_0}\right)^{p^\nu} = B_1^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \\ \vdots \\ \left(\frac{Y_n}{Y_0}\right)^{p^\nu} = B_n^{(c,a)}(t_1, \dots, t_{n-m}, \theta) \end{cases}$$

où θ est algébrique sur le corps $\overline{F}(t_1, \dots, t_{n-m})$, racine du polynôme $\phi^{(c,a)} \in \overline{F}(t_1, \dots, t_{n-m})[Z]$.

5.5 Coeur de l'induction

L'étape $m+1$ de l'induction consiste à partager de nouveau chaque U_m et à introduire le polynôme h_{m+1} (combinaison linéaire de f_1, \dots, f_k) pour calculer paramétriquement un point générique *efficace* et un système représentatif homogène pour chaque composante absolument irréductible $W_{w_m}^{(a)}$ de la variété $\mathcal{W}_{v_m}^{(a)} := W_{v_m}^{(a)} \cap V(h_{m+1}^{(a)})$ définie au section 2 ci-dessus (les w_m sont les fils des noeuds v_m qui ne sont pas des feuilles de l'arbre $T^{(a)}$).

5.5.1 Construction de h_{m+1}

Soit $a \in U_m$, alors par la définition de l'arbre $T^{(a)}$, la famille des variétés $W_{v_{m+1}}^{(a)}$ où v_{m+1} sont les noeuds de niveau $m+1$ coïncide avec la famille des composantes absolument irréductibles des variétés $W_{v_m}^{(a)}$ où v_m sont les noeuds du second type, de niveau m . Donc le polynôme $h_{m+1}^{(a)}$ ne doit pas s'annuler identiquement sur toutes les variétés $W_{v_m}^{(a)}$ où v_m sont les noeuds du second type, de niveau m .

La construction de h_{m+1} est basée sur le lemme 2.2.8 du chapitre 2 et le lemme suivant [58] :

Lemme 5.5.1 *Pour tout $a \in U_m$, le nombre des noeuds v_m de niveau m de l'arbre $T^{(a)}$ est inférieur ou égale à d^m .*

Preuve. Pour tout $1 \leq m \leq n$, les variétés $W_{v_m}^{(a)}$ (les v_m sont les noeuds, de niveau m) sont des composantes de la variété $V(h_1^{(a)}, \dots, h_m^{(a)})$ (corollaire 5.2.3) alors leur nombre est borné par $\deg V(h_1^{(a)}, \dots, h_m^{(a)}) \leq d^m$. \square

Proposition 5.5.2 *Soient $\mathcal{N} := (k-1)d^m + 1$ et $\alpha_1, \dots, \alpha_{\mathcal{N}} \in H$, \mathcal{N} éléments non-nuls de H distincts deux à deux. Pour tout $a \in U_m$, il existe un polynôme parmi $h_{\alpha_1}^{(a)}, \dots, h_{\alpha_{\mathcal{N}}}^{(a)}$ où pour tout $1 \leq s \leq \mathcal{N}$,*

$$h_{\alpha_s} := \sum_{1 \leq j \leq k} \alpha_s^{j-1} f_j$$

qui ne s'annule pas identiquement sur toutes les variétés $W_{v_m}^{(a)}$ où v_m sont les noeuds du second type, de niveau m .

Preuve. Sinon, par le lemme 5.5.1 et le principe de *Dirichlet*, il existe un noeud v_m du second type, de niveau m de $T^{(a)}$ et k éléments $\alpha_{s_1}, \dots, \alpha_{s_k}$ parmi $\alpha_1, \dots, \alpha_{\mathcal{N}}$, tel que $h_{\alpha_{s_1}}^{(a)}, \dots, h_{\alpha_{s_k}}^{(a)}$ s'annulent identiquement sur $W_{v_m}^{(a)}$. Alors $f_1^{(a)}, \dots, f_k^{(a)}$ s'annulent identiquement sur $W_{v_m}^{(a)}$ car $\alpha_{s_1}, \dots, \alpha_{s_k}$ sont deux à deux distincts, ceci en contradiction avec le fait que v_m est du second type. \square

Pour tout $1 \leq s \leq \mathcal{N}$, on pose

$$U_{m,s} = \{a \in U_m, \quad h_{\alpha_s}^{(a)} \text{ ne s'annule pas identiquement sur toutes les } W_{v_m}^{(a)}, v_m \text{ s.t.}\}$$

et

$$\tilde{U}_{m,s} = U_{m,s} \setminus \bigcup_{1 \leq s' < s} U_{m,s'}$$

où *s.t* est une abréviation de "second type".

Lemme 5.5.3 *Les ensembles $\tilde{U}_{m,s}$ ($1 \leq s \leq \mathcal{N}$) forment une partition de U_m . Chaque $U_{m,s}$ est un sous-ensemble constructible de U_m . Les degrés des équations et des inéquations qui le définissent par rapport à u (resp. T_1, \dots, T_l) sont bornés par*

$$\delta^{O(r)} d^{O(mrd^2)}$$

(resp. $\delta^{O(r)} d_1^{O(1)} d_2 d^{O(mrd^2)}$). Leurs tailles binaires sont bornées par

$$(M_1 + M_2) \delta^{O(r)} d_1^{O(1)} d_2 d^{O(mrd^2)}.$$

Preuve. Par le lemme 2.2.8 du chapitre 2, l'ensemble constructible $U_{m,s}$ est la réalisation de la formule quantifiée définie sur le corps $F(t_1, \dots, t_{n-m})$ par :

$$\exists C, \theta, \quad h_{\alpha_s} \left(1, B_1(C, \theta), \dots, B_n(C, \theta) \right) \neq 0, \quad \chi(C) = 0, \quad \phi(C, \theta) = 0$$

Ceci pour tous les noeuds v_m du second type. Le nombre des atomes de cette formule est borné par $3d^m$ (par le lemme 5.5.1), leurs degrés par rapport aux variables (C, θ) (resp. u et T_1, \dots, T_l) sont bornés par

$$\delta d^{O(md)}$$

(resp. $\delta^{O(r)} d^{O(mrd^2)}$ et $\delta^{O(r)} d_2 d^{O(mrd^2)}$). Leurs tailles binaires sont bornées par $(M_1 + M_2) \delta^{O(r)} d_2 d^{O(mrd^2)}$ en tenant compte des expressions et des bornes sur les degrés de $\chi, \phi, B_1, \dots, B_n$ donnés par les hypothèses de l'induction (voir section 4 ci-dessus). Ce qui prouve le lemme en appliquant l'algorithme d'élimination de quantificateurs de [24] (voir le chapitre 2 aussi). \square

5.5.2 Réduction au cas paramétrique zéro-dimensionnel

On s'intéresse dans ce paragraphe aux variétés

$$\begin{aligned} \mathcal{W}_{v_m}^{(a)} &= W_{v_m}^{(a)} \cap V(h_{\alpha_s}^{(a)}) \\ &= V(\psi_1^{(c,a)}, \dots, \psi_N^{(c,a)}, h_{\alpha_s}^{(a)}) \subset P^n(\bar{F}) \end{aligned}$$

pour tout noeud v_m de $T^{(a)}$ du second type et ceci pour tout $a \in \tilde{U}_{m,s}$. Puisque $h_{\alpha_s}^{(a)}$ ne s'annule pas identiquement sur la variété absolument irréductible $W_{v_m}^{(a)}$ alors $\dim(\mathcal{W}_{v_m}^{(a)}) = n - m - 1$ et la dimension de chaque composante $W_{w_m}^{(a)}$ de $\mathcal{W}_{v_m}^{(a)}$ est égale à $n - m - 1$ (Théorème de la dimension de l'intersection [125, 112, 101, 31]).

Fixons un ensemble $\tilde{U}_{m,s}$, le lemme suivant construit une base de transcendance commune des corps des fonctions rationnelles de toutes les composantes $W_{w_m}^{(a)}$:

Lemme 5.5.4 *Sous les hypothèses et les notations ci-dessus, on peut produire une partition finie de $\tilde{U}_{m,s}$ en (au plus) $d^{O(n)}$ ensembles \mathcal{V} . Pour chaque \mathcal{V} , il existe une transformation linéaire inversible Z_0, \dots, Z_n à coefficients dans H tel que pour tout $a \in \mathcal{V}$*

et pour tout noeud v_m du second type de $T^{(a)}$ on a :

i) Les variétés $W_{w_m}^{(a)}$ ne sont pas contenues dans l'hyperplan $V(Z_0)$.

ii) Les fonctions rationnelles $t_1 := \frac{Z_1}{Z_0}, \dots, t_{n-m-1} := \frac{Z_{n-m-1}}{Z_0}$ forment une base de transcendance commune de chaque composante $W_{w_m}^{(a)}$ de $\mathcal{W}_{v_m}^{(a)}$.

Preuve. Soit $a \in \tilde{U}_{m,s}$, puisque $\deg(\mathcal{W}_{v_m}^{(a)}) \leq d^{m+1}$ (par l'inégalité de Bézout), alors le lemme 5.3.2 assure l'existence d'un élément $(Z_0, \dots, Z_{n-m-1}) \in M := M_{n,n-m-1,d^{m+1}}$ qui vérifie

$$\mathcal{W}_{v_m}^{(a)} \cap V(Z_0, \dots, Z_{n-m-1}) = \emptyset.$$

Pour tout élément (Z_0, \dots, Z_{n-m-1}) de M , on associe un sous-ensemble \mathcal{V} de $\tilde{U}_{m,s}$ défini par :

$$\mathcal{V} := \left\{ a \in \tilde{U}_{m,s}, \quad \mathcal{W}_{v_m}^{(a)} \cap V(Z_0, \dots, Z_{n-m-1}) = \emptyset, \quad \text{pour tout } v_m \text{ s.t.} \right\}.$$

Ces ensembles forment une partition de $\tilde{U}_{m,s}$ et vérifient les points i) et ii) ci-dessus par le lemme 5.3.1 en complétant chaque Z_0, \dots, Z_{n-m-1} en une base Z_0, \dots, Z_n de l'espace de formes linéaires en Y_0, \dots, Y_n à coefficients dans H . \square

On fixe un certain ensemble \mathcal{V} du lemme 5.5.4 avec la base (Z_0, \dots, Z_n) correspondante. On peut écrire \mathcal{V} comme intersection des ensembles suivants (pour tous les noeuds v_m du second type) :

$$\mathcal{V}_{v_m} := \{a \in \tilde{U}_{m,s}, \quad \mathcal{W}_{v_m}^{(a)} \cap V(Z_0, \dots, Z_{n-m-1}) = \emptyset\}.$$

En exprimant Y_0, \dots, Y_n en fonction de cette base, on peut représenter chaque polynôme ψ_j comme un élément de $F(C, u_1, \dots, u_r)[Z_0, \dots, Z_n]$ et h_{α_s} comme un élément de $F[u_1, \dots, u_r, Z_0, \dots, Z_n]$. On fixe un certain noeud v_m , du second type et on considère le corps $F' := F(t_1, \dots, t_{n-m-1})$. On définit un système algébrique paramétré S_{v_m} par :

$$S_{v_m} : \begin{cases} \psi_j(Z_0, t_1 Z_0, \dots, t_{n-m-1} Z_0, Z_{n-m}, \dots, Z_n) = 0, & 1 \leq j \leq N \\ h_{\alpha_s}(Z_0, t_1 Z_0, \dots, t_{n-m-1} Z_0, Z_{n-m}, \dots, Z_n) = 0 \end{cases}$$

Pour tout $a \in \mathcal{V}$, on note par $S_{v_m}^{(a)}$ le système algébrique à coefficients dans $\overline{F'}$ obtenu à partir de S_{v_m} par évaluation de ses équations en (c, a) où c est une racine de $\chi^{(a)} \in \overline{F}[C]$. Ce système est zéro-dimensionnel dans $P^{m+1}(\overline{F'})$ et n'a pas de solutions à l'infini par le lemme 5.3.1. Par les hypothèses de l'induction, les degrés des équations de ce système par rapport à u et par rapport à T_1, \dots, T_l (resp. C et t_1, \dots, t_{n-m-1}) sont bornés par

$$d_2 \delta^{O(r)} d^{O(mrd^2)}$$

(resp. $\delta d^{O(md)}$ et $d^{O(m)}$). Leurs tailles binaires sont $\leq (M_1 + M_2) d_2 \delta^{O(r)} d^{O(mrd^2)}$. Leurs degrés par rapport à Z_0, Z_{n-m}, \dots, Z_n sont $\leq d^{O(m)}$. Leur nombre est $\leq d^{O(mn)}$

Théorème 5.5.5 *Sous les notations ci-dessus, il existe un algorithme qui partage chaque ensemble \mathcal{V}_{v_m} en*

$$(\delta dd_1)^{r^3 d^{O(m^2 n)}}$$

ensembles constuctibles \mathcal{E} vérifiant :

1) *Chaque \mathcal{E} est donné par des équations et des inéquations dans $F[u]$ de degrés par rapport à u et par rapport à T_1, \dots, T_l bornés par*

$$d_2 \delta^{O(r^3)} (dd_1)^{r^3 d^{O(m^2 n)}}.$$

Leurs tailles binaires sont bornées par $(M_1 + M_2) l d_2 \delta^{O(r^3)} (dd_1)^{r^3 d^{O(m^2 n)}}$.

2) *Pour chaque \mathcal{E} , l'algorithme calcule des polynômes $\mathcal{B}_{n-m}, \dots, \mathcal{B}_n \in F'(C, u)[Z]$ de degrés inférieurs ou égale à $d^{O(m^2)}$. Il calcule aussi un polynôme $\chi_2 \in F(u)[C]$ tel que pour toute spécialisation des paramètres $a \in \mathcal{E}$, il existe $c \in \overline{F}$, racine de $\chi_2^{(a)}$ qui vérifie :*

- *Aucun des dénominateurs des coefficients de $\mathcal{B}_{n-m}, \dots, \mathcal{B}_n$ ne s'annule en (c, a) .*

- *Les degrés des coefficients de $\mathcal{B}_{n-m}, \dots, \mathcal{B}_n$ par rapport à u et par rapport à T_1, \dots, T_l (resp. C et t_1, \dots, t_{n-m-1}) sont bornés par*

$$d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$$

(resp. $\delta d^{O(m^3 d)}$ et $d^{O(m^2 n)}$). Leurs tailles binaires sont bornées par $(M_1 + M_2) d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$

- *L'ensemble de solutions du système $S_{v_m}^{(a)}$ est divisé en (au plus) $d^{O(m^2 n)}$ classes \mathcal{S} de solutions. Pour chaque classe \mathcal{S} , l'algorithme calcule un polynôme $\Gamma \in F(C, u)[t_1, \dots, t_{n-m-1}, Z]$ tel qu'une représentation paramétrique des éléments de \mathcal{S} est donnée par*

$$\Gamma^{(c,a)}(\eta) = 0, \quad \begin{cases} \left(\frac{Z_{n-m}}{Z_0} \right)^{p^\mu} &= \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ \vdots & \\ \left(\frac{Z_n}{Z_0} \right)^{p^\mu} &= \mathcal{B}_n^{(c,a)}(\eta) \end{cases}$$

Les degrés des coefficients de Γ et χ_2 par rapport à u et par rapport à T_1, \dots, T_l (resp. C et t_1, \dots, t_{n-m-1}) sont bornés par

$$d_2 \delta^{O(r^3)} d^{r^3 d^{O(m^2 n)}}$$

(resp. $\delta^{O(r^2)} d^{r^2 d^{O(m^2 n)}}$ et $d^{O(m^2 n)}$). Leurs tailles binaires sont bornées par $(M_1 + M_2) d_2 \delta^{O(r^3)} d^{r^3 d^{O(m^2 n)}}$.

Preuve. Pour tout $a \in \mathcal{V}_{v_m}$, le système $S_{v_m}^{(a)}$ admet un nombre fini de solutions dans $P^{m+1}(\overline{F'})$ et n'a pas de solutions à l'infini, alors l'algorithme du théorème 3.5.3 du chapitre 3 permet d'obtenir une partition finie de \mathcal{V}_{v_m} en ensembles constructibles \mathcal{A} . Pour chaque \mathcal{A} , l'algorithme calcule de polynômes $\Lambda, \mathcal{B}_{n-m}, \dots, \mathcal{B}_n \in F'(C, u)[Z]$. Pour toute spécialisation $a \in \mathcal{A}$, il existe $c \in \overline{F}$, racine de $\chi^{(a)}$ tel qu'une représentation paramétrique de solutions du système $S_{v_m}^{(a)}$ est donnée par

$$\Lambda^{(c,a)}(\eta) = 0, \quad \begin{cases} \left(\frac{Z_{n-m}}{Z_0} \right)^{p^\mu} &= \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ &\vdots \\ \left(\frac{Z_n}{Z_0} \right)^{p^\mu} &= \mathcal{B}_n^{(c,a)}(\eta) \end{cases}$$

Les bornes sur les degrés et les tailles binaires des coefficients de $\mathcal{B}_{n-m}, \dots, \mathcal{B}_n$ ainsi que celles de Λ (voir le point 2 du théorème 5.5.5) se déduisent du théorème 3.5.3 en tenant compte de celles du système S_{v_m} ci-dessus.

Ecrivons Λ sous la forme $\Lambda = \frac{\Lambda_1}{\Lambda_2}$ où

$$\Lambda_1 \in F(C, u)[t_1, \dots, t_{n-m-1}, Z], \quad \Lambda_2 \in F[t_1, \dots, t_{n-m-1}]$$

avec $\deg_u(\Lambda_1) \leq \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$ et $\deg_{t_1, \dots, t_{n-m-1}, Z}(\Lambda_1) \leq d^{O(m^2 n)}$. Appliquons l'algorithme de factorisation absolue de polynômes paramétrés du chapitre 4 sur le polynôme Λ_1 où les variables sont t_1, \dots, t_{n-m-1}, Z . Cet algorithme partage chaque \mathcal{A} en un nombre fini d'ensembles constructibles \mathcal{G} .

Pour chaque \mathcal{G} , l'algorithme calcule au plus $d^{O(m^2 n)}$ polynômes $G \in F(C, u)[t_1, \dots, t_{n-m-1}, Z]$ et un polynôme $\chi_1 \in F(u)[C]$. Pour tout $a \in \mathcal{G}$, il existe $c \in \overline{F}$ racine de $\chi_1^{(a)}$ vérifiant :

$$\Lambda_1^{(c,a)} = \prod_G G^{(c,a)}, \quad G^{(c,a)} \text{ est absolument irréductible.}$$

Appliquons maintenant l'algorithme A2 du chapitre 2 pour calculer les p.g.c.d. paramétriques de χ et χ_1 dans $F(u)[C]$. Cet algorithme partage de nouveau chaque \mathcal{G} en un nombre fini d'ensembles constructibles \mathcal{E} . Pour chaque \mathcal{E} , l'algorithme calcule un polynôme $\chi_2 \in F(u)[C]$ tel que pour tout $a \in \mathcal{E}$, le polynôme $\chi_2^{(a)}$ est un p.g.c.d. de $\chi^{(a)}$ et $\chi_1^{(a)}$ dans $\overline{F}[C]$.

Pour chaque polynôme G , prenons

$$\Gamma := \frac{G}{\Lambda_2} \in F'(C, u)[Z]$$

Ces polynômes partagent l'ensemble de solutions du système $S_{v_m}^{(a)}$ au sens du point 2) du théorème 5.5.5. Le nombre totale des éléments de cette partition de \mathcal{V}_{v_m} ainsi que les bornes sur les degrés et les tailles binaires sont obtenus par le théorème 3.5.3, la section 6 du chapitre 4 et l'algorithme A2 du chapitre 2. \square

5.5.3 Construction d'un point générique efficace paramétrique de chaque composante $W_{w_m}^{(a)}$

Fixons un ensemble constructible \mathcal{E} du théorème 5.5.5, pour chaque couple $(c, a) \in \overline{F} \times \mathcal{E}$ où c est une racine de $\chi_2^{(a)}$, on considère l'anneau suivant de coordonnées de la variété affine $\mathcal{W}_{v_m}^{(a)} \cap \{Z_0 \neq 0\}$ sur \overline{F} :

$$\begin{aligned} A &= \overline{F}[\mathcal{W}_{v_m}^{(a)} \cap \{Z_0 \neq 0\}] \\ &= \overline{F}[Z_1, \dots, Z_n] / \left(\psi_1^{(c,a)}(1, Z_1, \dots, Z_n), \dots, \psi_N^{(c,a)}(1, Z_1, \dots, Z_n), h_{\alpha_s}^{(a)}(1, Z_1, \dots, Z_n) \right) \end{aligned}$$

Dans la suite nous allons établir une adaptation du lemme 2.5 de [58] au cas paramétrique pour élaborer une correspondance bijective entre les composantes absolument irréductibles $W_{w_m}^{(a)}$ de $\mathcal{W}_{v_m}^{(a)}$ et les classes $(\mathcal{S}, \Gamma^{(c,a)})$ du système $S_{v_m}^{(a)}$ (lemme 5.5.8 ci-dessous). Celle-ci permettra d'avoir un point générique *efficace* de chacune de ces composantes d'une manière uniforme (voir corollaire 5.5.9). Nous aurons besoin de deux lemmes suivants [125, 79].

Lemme 5.5.6 *Il existe une correspondance bijective entre l'ensemble des composantes absolument irréductibles de la variété $\mathcal{W}_{v_m}^{(a)}$ et l'ensemble des idéaux premiers minimaux de l'anneau A .*

Considérons l'ensemble multiplicatif $P = \overline{F}[Z_1, \dots, Z_{n-m-1}] \setminus \{0\} \subset A$. La localisation $P^{-1}A$ de A en P est un anneau local, i.e, admet un seul idéal maximal.

Lemme 5.5.7 *Les idéaux premiers minimaux de l'anneau $P^{-1}A$ sont de la forme $P^{-1}I$ où I est un idéal premier minimal de A qui n'intersecte pas P .*

Lemme 5.5.8 *Sous les notations ci-dessus, les trois ensembles suivants sont en bijection :*

- 1) *L'ensemble des composantes absolument irréductibles $W_{w_m}^{(a)}$ de la variété $\mathcal{W}_{v_m}^{(a)}$, i.e., l'ensemble des fils w_m du noeud v_m de l'arbre $T^{(a)}$.*
- 2) *L'ensemble de classes d'homomorphismes d'algèbres $P^{-1}A \longrightarrow \overline{F'}$ de même noyau sur le corps $F' = F(t_1, \dots, t_{n-m-1})$.*
- 3) *L'ensemble des classes $(\mathcal{S}, \Gamma^{(c,a)})$ du système $S_{v_m}^{(a)}$ (voir théorème 5.5.5).*

Preuve. 1) \Leftrightarrow 2) : Soit $W_{w_m}^{(a)}$ une composante absolument irréductible de $\mathcal{W}_{v_m}^{(a)}$ alors par le lemme 5.5.6, l'idéal $I_{w_m} := I(W_{w_m}^{(a)})$ est un idéal premier minimal de A . Puisque I_{w_m} n'intersecte pas P car Z_1, \dots, Z_{n-m-1} sont algébriquement indépendants dans l'anneau $\overline{F}[W_{w_m}^{(a)} \cap \{Z_0 = 1\}]$, alors par le lemme 5.5.7, $P^{-1}I_{w_m}$ est un idéal premier minimal de $P^{-1}A$.

Or $P^{-1}A$ est une algèbre de dimension finie sur $\overline{F}(t_1, \dots, t_{n-m-1})$ car le système $S_{v_m}^{(a)}$ admet un nombre fini de solutions dans $P^{m+1}(\overline{F'})$, alors $P^{-1}I_{w_m}$ est un idéal maximal

de $P^{-1}A$ et $F' \subset P^{-1}A/P^{-1}I_{w_m}$ est une extension finie des corps. Alors il existe un homomorphisme des corps

$$P^{-1}A/P^{-1}I_{w_m} \longrightarrow \overline{F'}$$

qui envoie Z_i en t_i pour tout $1 \leq i \leq n - m - 1$. Donc on associe à $W_{w_m}^{(a)}$ la classe d'homomorphismes de même noyaux engendré par la composition de cet homomorphisme avec la surjection canonique $P^{-1}A \longrightarrow P^{-1}A/P^{-1}I_{w_m}$.

Réciproquement, pour une classe d'homomorphismes, son noyau est un idéal maximal de $P^{-1}A$, par le lemme 5.5.7 il est de la forme $P^{-1}I$ où I est un idéal premier minimal de A qui n'intersecte pas P , il lui correspond une composante absolument irréductible de $\mathcal{W}_{v_m}^{(a)}$ par le lemme 5.5.6.

2) \Leftrightarrow 3) : Soit $\tau : P^{-1}A \longrightarrow \overline{F'}$ une classe d'homomorphismes sur F' , le point

$$\xi := (1, \tau(Z_{n-m}), \dots, \tau(Z_n))$$

est une solution du système $S_{v_m}^{(a)}$ alors il existe une certaine classe de solutions \mathcal{S} avec son polynôme associé $\Gamma^{(c,a)}$ tel que $\xi \in \mathcal{S}$ (théorème 5.5.5). Donc il existe une racine η de $\Gamma^{(c,a)} \in \overline{F'}[Z]$ tels que les équations

$$\begin{cases} \tau(Z_{n-m})^{p^\mu} &= \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ &\vdots \\ \tau(Z_n)^{p^\mu} &= \mathcal{B}_n^{(c,a)}(\eta) \end{cases}$$

nous donnent l'égalité suivante :

$$\overline{F'}[\eta] = \overline{F'}[\tau(Z_{n-m})^{p^\mu}, \dots, \tau(Z_n)^{p^\mu}]$$

on associe à τ la classe $(\mathcal{S}, \Gamma^{(c,a)})$.

Reciproquement, soit $(\mathcal{S}, \Gamma^{(c,a)})$ une classe de solutions du système $S_{v_m}^{(a)}$, on a l'égalité suivante des corps (par le point 2 du théorème 5.5.5) :

$$\overline{F'}[\eta] = \overline{F'}\left[\left(\frac{\xi_{n-m}}{\xi_0}\right)^{p^\mu}, \dots, \left(\frac{\xi_n}{\xi_0}\right)^{p^\mu}\right]$$

où η est une racine de $\Gamma^{(c,a)} \in \overline{F'}[Z]$ et $(\xi_0 : \xi_{n-m} : \dots : \xi_n) \in \mathcal{S}$. Il existe un homomorphisme de $\overline{F'}[\eta]$ dans $\overline{F'}$, celui-ci peut-être prolongé à un homomorphisme

$$\sigma : \overline{F'}\left[\frac{\xi_{n-m}}{\xi_0}, \dots, \frac{\xi_n}{\xi_0}\right] \longrightarrow \overline{F'}$$

car l'extension

$$\overline{F'}\left[\left(\frac{\xi_{n-m}}{\xi_0}\right)^{p^\mu}, \dots, \left(\frac{\xi_n}{\xi_0}\right)^{p^\mu}\right] \subset \overline{F'}\left[\frac{\xi_{n-m}}{\xi_0}, \dots, \frac{\xi_n}{\xi_0}\right]$$

est purement inséparable. Puisque $(\xi_0 : \xi_{n-m} : \dots : \xi_n)$ est une solution du système $S_{v_m}^{(a)}$ alors il existe un homomorphisme d'algèbre sur F' :

$$\pi : P^{-1}A \longrightarrow \overline{F'}\left[\frac{\xi_{n-m}}{\xi_0}, \dots, \frac{\xi_n}{\xi_0}\right]$$

Donc on associe l'homomorphisme $\sigma \circ \pi$ à cette classe de solutions. \square

Corollaire 5.5.9 *Sous les notations ci-dessus, on peut construire un point générique efficace pour chaque composante $W_{w_m}^{(a)}$ de la variété $\mathcal{W}_{v_m}^{(a)}$. Les bornes sur les degrés et les tailles binaires des expressions qui interviennent dans la représentation du point générique efficace sont comme dans le théorème 5.2.5.*

Preuve. Soit w_m un fils de v_m , par le lemme 5.5.8, on associe une classe $(\mathcal{S}, \Gamma^{(c,a)})$ de solutions du système $S_{v_m}^{(a)}$ et un homomorphisme de F' -algèbre

$$\sigma : P^{-1}A \longrightarrow \overline{F'}$$

de noyau $P^{-1}I_{w_m}$. Il existe donc un homomorphisme $P^{-1}A/P^{-1}I_{w_m} \longrightarrow \overline{F'}$, ceci nous donne l'égalité

$$\overline{F'}[\eta] = \overline{F'}\left[\sigma(Z_{n-m})^{p^\mu}, \dots, \sigma(Z_n)^{p^\mu}\right]$$

où η est une racine de $\Gamma^{(c,a)}$. D'où l'isomorphisme de corps suivant qui définit un point générique efficace de la composante $W_{w_m}^{(a)}$:

$$\overline{F'}[\eta] \simeq \overline{F}\left(\frac{Z_1}{Z_0}, \dots, \frac{Z_{n-m-1}}{Z_0}, \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu}, \dots, \left(\frac{Z_n}{Z_0}\right)^{p^\mu}\right) \subset \overline{F}(W_{w_m}^{(a)}).$$

Cet isomorphisme est défini par les expressions suivantes :

$$\Gamma^{(c,a)}(\eta), \quad \left\{ \begin{array}{ll} \frac{Z_1}{Z_0} & = t_1 \\ \vdots & \\ \frac{Z_{n-m-1}}{Z_0} & = t_{n-m-1} \\ \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu} & = \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ \vdots & \\ \left(\frac{Z_n}{Z_0}\right)^{p^\mu} & = \mathcal{B}_n^{(c,a)}(\eta) \end{array} \right.$$

Les bornes sur les degrés et les tailles binaires de polynômes $\mathcal{B}_{n-m}, \dots, \mathcal{B}_n$ et Γ sont données par le théorème 5.5.5. \square

5.5.4 Construction d'un système représentatif paramétrique de chaque composante $W_{w_m}^{(a)}$

Fixons dans ce paragraphe un ensemble constructible \mathcal{E} du théorème 5.5.5 et un fils w_m du noeud v_m , de second type. Nous voulons dans ce paragraphe partager de nouveau \mathcal{E} en un nombre fini d'ensembles constructibles. Pour chacun d'eux, nous calculons de polynômes $\Psi_1, \dots, \Psi_M \in F(C, u)[Z_0, \dots, Z_n]$ homogène en Z_0, \dots, Z_n tels que leurs spécialisations en (c, a) définissent la variété $W_{w_m}^{(a)}$ pour toute valeur a des paramètres dans cet ensemble et c une racine de $\chi_2^{(a)}$ (voir le lemme 5.5.12).

On associe au fils w_m un \overline{F} -sous-espace vectoriel, noté Ω_{w_m} , de l'espace de tous les polynômes homogènes de $\overline{F}[Z_0, \dots, Z_n]$ de degrés d^{m+1} par :

$$\Omega_{w_m} := \{g \in \overline{F}[Z_0, \dots, Z_n], \text{ homogène, } \deg(g) = d^{m+1}, \quad g \equiv 0 \text{ sur } W_{w_m}^{(a)}\}.$$

Il est évident que $W_{w_m}^{(a)} \subset V(\Omega_{w_m})$ où $V(\Omega_{w_m}) \subset P^n(\overline{F})$ est l'ensemble des zéros communs des polynômes de Ω_{w_m} . Pour montrer l'égalité entre ces deux variétés, nous aurons besoin du lemme suivant [66, 58] :

Lemme 5.5.10 *Soient $W_1 \subset W_2 \subset P^n(\overline{F})$ deux variétés projectives avec $\deg(W_1) \leq d$. Alors il existe un polynôme homogène $g \in \overline{F}[Z_0, \dots, Z_n]$ de degré $\leq d$ qui s'annule identiquement sur W_1 . En plus, pour toute composante absolument irréductible W_3 de W_2 qui n'est pas une composante absolument irréductible de W_1 on a $\dim(W_3 \cap V(g)) = \dim(W_3) - 1$.*

Proposition 5.5.11

$$W_{w_m}^{(a)} = V(\Omega_{w_m}).$$

Preuve. Supposons que $V(\Omega_{w_m}) \not\subset W_{w_m}^{(a)}$ alors il existe un élément $\xi \in V(\Omega_{w_m})$ et $\xi \notin W_{w_m}^{(a)}$. Appliquons le lemme 5.5.10 sur les deux variétés $W_1 := W_{w_m}^{(a)}$ et $W_2 := W_{w_m}^{(a)} \cup \{\xi\}$, puisque $\deg(W_{w_m}^{(a)}) \leq \deg(W_{w_m}^{(a)}) \leq d^{m+1}$ alors il existe un polynôme $g \in \Omega_{w_m}$ et par suite $g(\xi) = 0$, donc g s'annule identiquement sur W_2 et pour toute composante absolument irréductible W_3 de W_2 , on a $W_3 \cap V(g) = W_3$, ceci est une contradiction avec le lemme 5.5.10. \square

Lemme 5.5.12 *Sous les hypothèses ci-dessus, il existe un algorithme qui partage \mathcal{E} en (au plus) $d^{O(m^2 n^2)}$ ensembles constructibles \mathcal{U} . Pour chaque \mathcal{U} , l'algorithme calcule un système représentatif paramétrique $\Psi_1, \dots, \Psi_M \in F(C, u)[Z_0, \dots, Z_n]$ de W_{w_m} . Les bornes sur les degrés et les tailles binaires de ces polynômes sont comme dans le théorème 5.2.5.*

Preuve. Soit $(c, a) \in \overline{F} \times \mathcal{E}$ où c est une racine de $\chi_2^{(a)}$, la proposition 5.5.11 montre que si $\{g_1, \dots, g_M\}$ est une base de Ω_{w_m} alors

$$W_{w_m}^{(a)} = V(g_1, \dots, g_M)$$

où

$$M := \dim_{\overline{F}}(\Omega_{w_m}) \leq \binom{n + d^{m+1}}{n} \leq (3d^{m+1})^n \leq d^{O(mn)}.$$

Remarquons que par le lemme 2.2.8 du chapitre 2, un polynôme $g \in \overline{F}[Z_0, \dots, Z_n]$, de degré d^{m+1} est un élément de Ω_{w_m} si et seulement si

$$g\left(1, t_1, \dots, t_{n-m-1}, \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu}, \dots, \left(\frac{Z_n}{Z_0}\right)^{p^\mu}\right) = 0 \quad \text{dans} \quad \overline{F}(t_1, \dots, t_{n-m-1})[\eta]$$

où les expressions des fonctions rationnelles $\left(\frac{Z_t}{Z_0}\right)^{p^\mu}$ sont données par l'isomorphisme du preuve du corollaire 5.5.9 qui définit un point générique *efficace* de $W_{w_m}^{(a)}$.

Cette équation définit un système linéaire homogène paramétré obtenu en mettant tous ses coefficients en $t_1, \dots, t_{n-m-1}, \eta$ égaux à zéros. Le degré de cette équations par rapport à $t_1, \dots, t_{n-m-1}, \eta$ est $\leq d^{O(m^2n)}$, alors le nombre d'équations de ce système est borné par

$$(d^{O(m^2n)})^{(n-m)} \leq d^{O(m^2n^2)}$$

Les inconnues de ce système sont les coefficients de g , leur nombre est

$$\binom{n + d^{m+1}}{n} \leq (3d^{m+1})^n \leq d^{O(mn)}.$$

Les degrés des équations de ce système par rapport à u et par rapport à T_1, \dots, T_l (resp. C) sont bornés par

$$d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$$

(resp. $\delta d^{O(m^3 d)}$) (voir théorème 5.5.5). Grâce au lemme 5.5.10, ce système vérifie la propriété suivante :

Pour tout $a \in \mathcal{E}$, il existe $c \in \overline{F}$ racine de $\chi_2^{(a)} \in \overline{F}[C]$ tel que le système homogène à coefficients dans \overline{F} obtenu après évaluation des variables C et u en c et a respectivement admet une solution non triviale.

On applique l'algorithme de Gauss paramétrique du chapitre 2 sur ce système, ce qui permet de décomposer \mathcal{E} en (au plus) $d^{O(m^2n^2)}$ ensembles constructibles \mathcal{U} vérifiant :

- Les degrés des équations et des inéquations de chaque \mathcal{U} par rapport à u et par rapport à T_1, \dots, T_l sont bornés par

$$d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}.$$

- Pour chaque \mathcal{U} , l'algorithme calcule des polynômes $\Psi_1, \dots, \Psi_M \in F(C, u)[Z_0, \dots, Z_n]$ qui vérifient :

1) $\deg_C(\Psi_j) \leq \delta d^{O(m^3 d)}$, $\deg_u(\Psi_j) \leq \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$ et $\deg_{T_1, \dots, T_l}(\Psi_j) \leq d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$ pour tout $1 \leq j \leq M$.

2) Pour tout $a \in \mathcal{U}$, il existe $c \in \overline{F}$ racine de $\chi_2^{(a)} \in \overline{F}[C]$ tels que :

- Aucun des dénominateurs de Ψ_1, \dots, Ψ_M ne s'annule en (c, a) .

- Les vecteurs des coefficients de $\Psi_1^{(c,a)}, \dots, \Psi_M^{(c,a)} \in \overline{F}[Z_0, \dots, Z_n]$ forment une base de l'espace Ω_{w_m} de solutions du système homogène correspondant. Ceci est équivalent à dire par la proposition 5.5.11 que

$$W_{w_m}^{(a)} = V(\Psi_1^{(c,a)}, \dots, \Psi_M^{(c,a)}) \subset P^n(\overline{F}). \square$$

5.6 Analyse de la complexité totale de l'algorithme du théorème 5.2.5

Le nombre totale d'éléments de cette partition finie de l'espace des paramètres ainsi que les bornes sur leurs degrés et leurs tailles binaires double-exponentielle (en n) (voir théorème 5.2.5) s'obtiennent des hypothèses de l'induction (section 4), du lemme 5.5.3, lemme 5.5.4, théorème 5.5.5 et du lemme 5.5.12.

Nous analysons la complexité de l'étape $m + 1$ de l'induction, en effet, la complexité de la construction des $\mathcal{N} = (k - 1)d^m + 1$ ensembles $\tilde{U}_{m,s}$ est juste celle de l'algorithme d'élimination de quantificateurs de [24] appliqué sur la formule décrite dans la preuve du lemme 5.5.3, elle est donc bornée par

$$(\delta d_1 d_2)^{O(r^2 l)} d^{O(m r^2 l d^2)}.$$

La complexité du calcul de tous les ensembles constuctibles \mathcal{E} du théorème 5.5.5 est déterminée par celles de l'algorithme de résolution de systèmes paramétrés zéro-dimensionnels du chapitre 3 sur le système S_{v_m} définis ci-dessus et de l'algorithme de factorisation absolue de polynômes paramétrés du chapitre 4. En tenant compte des bornes établies dans la preuve du théorème 5.5.5 sur les degrés et les tailles binaires des entrées de ces algorithmes, cette complexité est donnée par

$$(\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(m^2 n)}}.$$

Cette borne est doublement exponentielle en $m^2 n$ vu que celle de l'algorithme de factorisation absolue de polynômes paramétrés du paragraphe 6 du chapitre 4 est exponentielle en le degré du polynôme à factoriser (ici ce degré est $d^{O(m^2 n)}$).

D'où la complexité de l'étape $m + 1$ de l'algorithme est bornée par

$$(\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(m^2 n)}}.$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} (\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(m^2 n)}}.$$

Remarque 5.6.1 *Le passage de l'étape m à l'étape $m + 1$ entraîne un passage des bornes (sur les degrés et sur le nombre des ensembles constructibles) exponentielles aux celles doublement exponentielles. Vu cette croissance on peut penser que puisqu'on a n étapes à parcourir pendant l'induction pour décrire toutes les variétés absolument irréductibles associées aux noeuds des arbres T , les bornes deviennent n - fois exponentielles en n à la dernière étape de l'induction. En fait, ceci n'arrive pas parce que dans chaque étape de l'induction, le degré du polynôme paramétré Λ_1 à factoriser (voir la preuve du théorème 5.5.5) reste toujours borné par $d^{O(m^2 n)}$. Donc toutes les bornes de la sortie de l'algorithme sont doublement exponentielles en n . De même, la complexité totale de l'algorithme est*

$$(\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(n^3)}}.$$

en tant que nombre d'opérations dans H . Sa complexité binaire est

$$(pM_1 M_2)^{O(1)} (\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(n^3)}}.$$

5.7 Description des composantes des variétés $V^{(a)}$

Revenons maintenant à la description des composantes absolument irréductibles des variétés $V^{(a)} = V(f_1^{(a)}, \dots, f_k^{(a)})$ d'une manière uniforme sur les valeurs des paramètres. Par la proposition 5.2.4, ces composantes sont parmi les variétés $W_{v_m}^{(a)}$ associées aux noeuds v_m des arbres des composantes $T^{(a)}$ (i.e., les feuilles de $T^{(a)}$).

Corollaire 5.7.1 *Chaque élément \mathcal{U} de la partition finie de l'espace des paramètres en ensembles constructibles du théorème 5.2.5 vérifie :*

- *Le nombre des composantes absolument irréductibles est constant sur \mathcal{U} , i.e., pour tout $a, b \in \mathcal{U}$, le nombre des composantes absolument irréductibles de la variété $V^{(a)}$ est égale à celui de $V^{(b)}$.*
- *Chaque composante absolument irréductible $W^{(a)}$ de $V^{(a)}$ est donné par un point générique efficace paramétrique et un système représentatif paramétrique. Les bornes sur les degrés et les tailles binaires des expressions qui interviennent dans leurs représentations sont comme dans le théorème 5.2.5.*

Preuve. Par le lemme 2.2.8 du chapitre 2, on peut vérifier si une variété $W_{v_m}^{(a)}$ de l'arbre $T^{(a)}$ donnée par un point générique efficace, est une composante de $V^{(a)}$. Les autres points de ce corollaire se déduisent du théorème 5.2.5. \square

Chapitre 6

Appendice

6.1 Notions de complexité

Nous utilisons deux sortes de complexité, la complexité algébrique comme étant le nombre d'opérations élémentaires dans le corps de base F et la complexité binaire en tenant compte de la représentation des éléments de F (voir aussi [118]).

6.1.1 Complexité binaire

Définition 6.1.1 1) La longueur d'un élément $a \in F_{p^m}$ est égale à $\log_2 p^m$.

2) Soit $a \in \mathbb{Z} \setminus \{0\}$, si $a = (-1)^\epsilon \sum_{0 \leq i \leq n} a_i 2^i$ est la représentation binaire de a avec $a_n = 1$, $a_i \in \{0, 1\}$ alors la longueur (taille binaire) de a , notée $l(a)$ est définie par :

$$l(a) = n + 1 = \lfloor \log_2 |a| \rfloor + 1 \leq \log_2 |a| + 1, \quad l(0) = 1$$

où $\lfloor * \rfloor$ est la partie entière de $*$.

3) La longueur (taille binaire) d'un polynôme $f \in \mathbb{Z}[X_1, \dots, X_n]$, notée $l(f)$, est le maximum des longueurs (tailles binaires) de ses coefficients dans \mathbb{Z} .

Proposition 6.1.2 (Propriétés des tailles binaires)

i) Si $a, b \in \mathbb{Z} \setminus \{0\}$ alors

$$l(a + b) \leq \max \{l(a), l(b)\}$$

et

$$l(a) + l(b) - 1 \leq l(ab) \leq l(a) + l(b)$$

ii) Si $f, g \in \mathbb{Z}[X_1, \dots, X_n]$ alors $l(f + g) \leq \max \{l(f), l(g)\} + 1$ et $l(fg) \leq l(f) + l(g) + 1$.

6.1.2 Symboles de complexité

Définition 6.1.3 Soient $f(k)$ et $g(k)$ deux fonctions positives.

1) On dit que $f(k)$ est un $O(g(k))$ (ou bien $f(k) = O(g(k))$) s'il existe une constante $c > 0$ et un élément k_0 tels que pour tout $k \geq k_0$ on ait $f(k) \leq cg(k)$.

2) On dit que $f(k)$ est un $\Omega(g(k))$ (ou bien $f(k) = \Omega(g(k))$) s'il existe une constante $c > 0$ et un élément k_0 tels que pour tout $k \geq k_0$ on ait $f(k) \geq cg(k)$.

3) On dit que $f(k)$ est un $\Theta(g(k))$ (ou bien $f(k) = \Theta(g(k))$) si et seulement si $f(k) = O(g(k))$ et $f(k) = \Omega(g(k))$.

4) On dit que $f(k)$ est un $o(g(k))$ (ou bien $f(k) = o(g(k))$) si pour tout $\epsilon > 0$ il

existe un élément k_0 tel que pour tout $k \geq k_0$ on ait $f(k) \leq \epsilon g(k)$. Ceci est équivalent à que

$$\lim_{k \rightarrow +\infty} \frac{f(k)}{g(k)} = 0.$$

5) On dit que $f(k)$ est un $\omega(g(k))$ (ou bien $f(k) = \omega(g(k))$) si pour tout $\epsilon > 0$ il existe un élément k_0 tel que pour tout $k \geq k_0$ on ait $f(k) \geq \epsilon g(k)$. Ceci est équivalent à que

$$\lim_{k \rightarrow +\infty} \frac{f(k)}{g(k)} = +\infty.$$

Définition 6.1.4 1) Un algorithme est dit *polynomial* (i.e., effectuant un calcul dans un temps polynomial) si sa complexité (i.e., temps d'exécution) est de la forme $k^{O(1)}$ où k est la taille de son entrée.

2) Un algorithme est dit *exponentiel* si sa complexité est un $e^{O(k)}$ où k est la taille de son entrée.

3) Un algorithme est dit *sous-exponentiel* si sa complexité est un $O(e^{f(k)})$ où $f(k)$ est un $o(k)$ et k est la taille de son entrée. Par exemple, $f(k) = \frac{k}{\log(\log(k))}$.

6.1.3 Complexité d'évaluation des polynômes multivariés

La complexité d'évaluation d'un polynôme multivarié est donnée par le lemme suivant :

Lemme 6.1.5 Soit $h \in F[X_1, \dots, X_n]$ un polynôme non nul de degré $\leq d$ et $(t_1, \dots, t_n) \in F^n$. Alors l'évaluation de h en (t_1, \dots, t_n) (i.e., le calcul de $h(t_1, \dots, t_n)$) se fait avec $\binom{n+d}{n} \leq (d+1)^n$ opérations élémentaires dans F . Si $F = \mathbb{Z}$ et $l(h), l(t_i) \leq M$ pour tout $1 \leq i \leq n$ alors la taille binaire de $h(t_1, \dots, t_n)$ est

$$l(h(t_1, \dots, t_n)) \leq (M+1)d.$$

6.2 Algèbre linéaire

Nous rassemblons dans cette section quelques lemmes (voir [118, 8]) qui sont utilisés dans les chapitres précédents.

Soit $F[X_1, \dots, X_n]_{\leq d}$ le F -sous-espace de $F[X_1, \dots, X_n]$ formé par les polynômes de degré total borné par d . Le lemme suivant montre que $F[X_1, \dots, X_n]_{\leq d}$ est de dimension finie sur F et calcule sa dimension.

Lemme 6.2.1 Le nombre des monômes de $F[X_1, \dots, X_n]$ de degré $\leq d$ est $\binom{n+d}{n} \leq (d+1)^n$.

Corollaire 6.2.2 *Le nombre des monômes de $F[X_0, \dots, X_n]$ de degré d est $\binom{n+d}{n}$.*

Lemme 6.2.3 *Soit A une matrice carrée d'ordre m à coefficients dans $F[X_1, \dots, X_n]$ de degré borné par d . Soit $D = \det(A) \in F[X_1, \dots, X_n]$. Alors*

$$\deg(D) \leq md.$$

6.3 Théorie combinatoire

6.3.1 Partitions des entiers

Définition 6.3.1 *Soit d un entier non nul. Une partition de d est une famille $\{d_1, \dots, d_s\}$ d'entiers qui vérifient :*

$$d = d_1 + \dots + d_s, \quad d_1 \geq \dots \geq d_s.$$

On note par $pt(d)$ l'ensemble des partitions de d .

Lemme 6.3.2 *Pour tout entier naturel d , le nombre d'éléments de $pt(d)$ est borné par d^{d+1} .*

Preuve. Le nombre d'éléments de $pt(d)$ est borné par

$$\begin{aligned} \sum_{2 \leq s \leq d} \binom{d-1+s-1}{s} &\leq \sum_{2 \leq s \leq d} (d-1)^s \\ &\leq \frac{(d-1)^{d-1} - 1}{d-2} (d-1)^2 \\ &\leq d^{d+1}. \square \end{aligned}$$

Une meilleure borne sur le nombre d'éléments de $pt(d)$ est donnée dans [3], à savoir 24^d .

6.3.2 Principe de Dirichlet

Rappelons ici un principe de la théorie combinatoire appelé le principe de Dirichlet, qui est énoncé par le mathématicien allemand Dirichlet en 1842 de la façon suivante :

Si n éléments sont distribués dans m ensembles et si m est strictement inférieur à n , alors il y a au moins un ensemble qui reçoit au moins deux éléments.

Une autre forme de ce principe s'énonce ainsi : si n éléments sont distribués dans n ensembles sans qu'il y en ait deux dans un même ensemble, alors chaque ensemble contient exactement un élément.

6.4 Variétés projectives

Soit F un corps commutatif et K une extension de F . L'espace $P^n = P^n(K) := (K^{n+1} \setminus \{0\}) / \sim$ est appelé l'espace projective n -dimensionnelle sur le corps K où \sim est la relation d'équivalence définie par :

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \in K \setminus \{0\}, (x_0, \dots, x_n) = \lambda(y_0, \dots, y_n)$$

Pour un élément $(x_0, \dots, x_n) \in K^{n+1} \setminus \{0\}$, sa classe d'équivalence modulo \sim est notée par $(x_0 : \dots : x_n)$, i.e.,

$$(x_0 : \dots : x_n) := \{\lambda(x_0, \dots, x_n), \lambda \in K \setminus \{0\}\}.$$

Définition 6.4.1 Un polynôme $f \in F[X_0, \dots, X_n]$ est dit homogène de degré d si tous ses monômes ont le même degré d .

Proposition 6.4.2 Tout polynôme $g \in F[X_0, \dots, X_n]$ s'écrit d'une manière unique sous la forme

$$g = \sum_{0 \leq i \leq d} g_i$$

où $d = \deg(g)$ est le degré total de g et $g_i \in F[X_0, \dots, X_n]$ est homogène de degré i pour tout $0 \leq i \leq d$. Les polynômes g_i sont appelés les composantes homogènes de g .

Proposition 6.4.3 Soit $f \in F[X_0, \dots, X_n]$ un polynôme homogène et $a = (a_0 : \dots : a_n) \in P^n(K)$. Si f s'annule en (a_0, \dots, a_n) alors f s'annule en $\lambda(a_0, \dots, a_n)$ pour tout $\lambda \in K \setminus \{0\}$.

Preuve. Il suffit de remarquer que $f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n)$ pour tout $\lambda \in K \setminus \{0\}$ où $d = \deg(f)$. \square

Définition 6.4.4 Soient $f_1, \dots, f_k \in F[X_0, \dots, X_n]$ de polynômes homogènes. L'ensemble

$$V_K(f_1, \dots, f_k) := \{(a_0 : \dots : a_n) \in P^n(K), f_i(a_0, \dots, a_n) = 0, \text{ pour tout } 1 \leq i \leq k\}$$

est appelé une F -variété projective de $P^n(K)$ définie par f_1, \dots, f_k .

Définition 6.4.5 Un idéal I de $F[X_0, \dots, X_n]$ est dit homogène si pour tout $g \in I$, ses composantes homogènes sont aussi dans I .

Théorème 6.4.6 Soit I un idéal de $F[X_0, \dots, X_n]$. Les propriétés suivantes sont équivalentes :

- i) I est un idéal homogène de $F[X_0, \dots, X_n]$.
- ii) $I = (f_1, \dots, f_k)$ où f_1, \dots, f_k sont de polynômes homogènes de $F[X_0, \dots, X_n]$.

Corollaire 6.4.7 Soit I un idéal homogène de $F[X_0, \dots, X_n]$. L'ensemble

$$V_K(I) := \{a \in P^n(K), f(a) = 0 \text{ pour tout } f \in I\}$$

est une F -variété projective.

Proposition 6.4.8 Soit $V \subset P^n(K)$ une F -variété projective et $I_F(V)$ l'ensemble défini par

$$I_F(V) := \{f \in F[X_0, \dots, X_n], f(a) = 0 \text{ pour toute } a \in V\}.$$

Si K est un corps infini alors $I_F(V)$ est un idéal homogène de $F[X_0, \dots, X_n]$.

Définition 6.4.9 Une F -variété projective $V \subset K^n$ est dite irréductible sur F si V ne peut pas être décomposée en union de deux F -variétés propres i.e., si $V = V_1 \cup V_2$ où V_1 et V_2 sont deux F -variétés alors $V_1 = V$ ou $V_2 = V$.

Définition 6.4.10 Une F -variété $V \subset K^n$ est dite absolument irréductible si elle est irréductible sur \overline{F} .

Théorème 6.4.11 Toute variété projective $V \subset P^n(K)$ s'écrit d'une manière unique sous la forme :

$$V = V_1 \cup \dots \cup V_m$$

où V_i est une variété projective irréductible avec $V_i \not\subset V_j$ pour tout $i \neq j$. Les variétés V_1, \dots, V_m sont appelées les composantes irréductibles de V .

6.4.1 Dimension

Dans la littérature, on trouve plusieurs définitions équivalentes de la dimension, notée $\dim V$, d'une variété algébrique V . Nous illustrons dans ce paragraphe une telle définition.

1- Indépendance algébrique :

Tout au long de ce paragraphe E désigne une extension de F .

Définition 6.4.12 Des éléments $\alpha_1, \dots, \alpha_r \in E$ sont dits algébriquement indépendants sur F s'il n'existe pas un polynôme non nul à r variables et à coefficients dans F qui s'annule en $(\alpha_1, \dots, \alpha_r) \in E^r$.

Définition 6.4.13 E est dite une extension purement transcendante de F s'il existe une famille finie $\alpha_1, \dots, \alpha_r$ d'éléments de E , algébriquement indépendants sur F tel que $E = F(\alpha_1, \dots, \alpha_r)$.

Proposition 6.4.14 Soit $\alpha_1, \dots, \alpha_r \in E$ algébriquement indépendants sur F et $\alpha \in E$. Alors $\alpha_1, \dots, \alpha_r, \alpha$ sont algébriquement indépendants sur F si et seulement si α est transcendant sur $F(\alpha_1, \dots, \alpha_r)$.

Définition 6.4.15 Une famille $B = \{\alpha_1, \dots, \alpha_r\}$ d'éléments de E est une base de transcendance de l'extension E/F si et seulement si :

i) $\alpha_1, \dots, \alpha_r$ sont algébriquement indépendants sur F .

ii) B est maximale avec la propriété i), i.e., B n'est pas strictement contenue dans aucune famille B' d'éléments de E , algébriquement indépendants sur F .

Corollaire 6.4.16 Soit $B = \{\alpha_1, \dots, \alpha_r\} \subset E$ tel que $\alpha_1, \dots, \alpha_r$ sont algébriquement indépendants sur F . Alors B est une base de transcendance de E/F si et seulement si E est une extension algébrique de $F(\alpha_1, \dots, \alpha_r)$.

Théorème 6.4.17 i) Ils existent des bases de transcendance de l'extension E/F .

ii) Deux bases de transcendance de E/F ont le même cardinal.

Définition 6.4.18 Le cardinal commun de toutes les bases de transcendance de E/F est appelé le degré de transcendance de E/F , noté $\deg tr_F E$.

Proposition 6.4.19 E est une extension algébrique de F si et seulement si $\deg tr_F E = 0$.

Théorème 6.4.20 Soit $F \subset E \subset L$ une suite d'extensions. Alors

$$\deg tr_F L = \deg tr_E L + \deg tr_F E.$$

2- Dimension d'une variété irréductible :

Soit V une F -variété affine de F^n , irréductible sur F . Le corps des fonctions rationnelles $F(V)$ est une extension de F .

Définition 6.4.21 La dimension de V , notée $\dim V$, est le degré de transcendance de $F(V)/F$, i.e., $\dim V$ est le nombre maximal d'éléments de $F(V)$ qui sont algébriquement indépendants sur F .

Définition 6.4.22 Si V est une F -variété de F^n , $\dim V$ est le maximum des dimensions des composantes irréductibles de V .

Définition 6.4.23 La codimension d'une variété algébrique V , notée $\text{codim} V$, est égale à $n - \dim V$.

Proposition 6.4.24 1) Soit V_1 et V_2 deux variétés algébriques. Si $V_1 \subset V_2$ alors $\dim V_1 \leq \dim V_2$.

2) Si F est algébriquement clos et $f \in F[X_0, \dots, X_n]$ un polynôme homogène non-constant. Alors $\dim V(f) = n - 1$.

Théorème 6.4.25 (Théorème de la dimension de l'intersection)

Supposons que F est algébriquement clos et $f_1, \dots, f_k \in F[X_0, \dots, X_n]$ de polynômes homogènes. Alors $\dim V(f_1, \dots, f_k) \geq n - k$.

Proposition 6.4.26 Soit V une variété algébrique.

1) V est un ensemble fini si et seulement si $\dim V = 0$.

2) $V = \emptyset$ si et seulement si $\dim V = -1$.

Théorème 6.4.27 Supposons que F est algébriquement clos et $V \subset P^n(F)$ une variété irréductible sur F . Soit $f \in F[X_0, \dots, X_n]$ un polynôme homogène qui ne s'annule pas sur V alors $\dim(V \cap V(f)) = \dim V - 1$ et la dimension de chaque composante de la variété $V \cap V(f)$ est $\dim V - 1$.

3- Base de transcendance d'une variété algébrique :

Définition 6.4.28 Une base de transcendance d'une variété V définie et irréductible sur F est une base de transcendance de son corps des fonctions rationnelles $F(V)$ sur F .

Soit $V = V(I) \subset P^n(K)$ une variété projective définie par l'idéal homogène $I = (g_1, \dots, g_s) \subset F[X_0, \dots, X_n]$, de codimension m .

Les bases de Gröbner permettent de calculer la dimension de V et éventuellement de calculer une base de transcendance :

Des variables X_0, \dots, X_l sont algébriquement indépendantes sur F si et seulement si $I \cap F[X_0, \dots, X_l] = \{0\}$. Cette dernière condition peut-être tester par un calcul d'une base de Gröbner G de I en respectant l'ordre lexicographique $X_0 \geq \dots \geq X_l \geq \dots \geq X_n$, parce que $G \cap F[X_0, \dots, X_l]$ est une base de Gröbner de $I \cap F[X_0, \dots, X_l]$ (voir [31, 98]).

6.4.2 Degré

Définition 6.4.29 Soit V une variété affine et irréductible, de dimension r . Le degré (géométrique) de V , noté $\deg(V)$, est défini par (voir [66])

$$\begin{aligned} \deg(V) &= \sup\{\#V \cap L_1 \cap \dots \cap L_r; \quad L_1, \dots, L_r \text{ hyperplans et } V \cap L_1 \cap \dots \cap L_r \text{ est fini}\} \\ &= \sup\{V \cap H; \quad H \text{ sous espace de } F^n \text{ de dimension } n - r, V \cap H \text{ est fini}\}. \end{aligned}$$

Définition 6.4.30 Soit V une variété affine. Le degré de V est la somme de degrés de ses composantes irréductibles.

Théorème 6.4.31 (Inégalité de Bézout [66, 15, 125, 112, 31]. Soient V_1 et V_2 deux variétés algébriques, une borne supérieure du degré de $V_1 \cap V_2$ est donnée par

$$\deg(V_1 \cap V_2) \leq \deg(V_1) \deg(V_2).$$

Bibliographie

- [1] A.V. Aho, J.E.H. Hopcroft, J.D. Ullman, *The design and analysis of computer algorithms*, Reading, Mass., Menlo Park, Cal., London, Addison-Wesley Publishing Company, 1974.
- [2] M.E. Alonso, E. Becker, M.-F. Roy and T. Wormann, *Zeros, multiplicities and idempotents for zero-dimensional systems*, Algorithms in algebraic geometry and applications, 1996, p. 1-15.
- [3] Andrews, G. E. *The theory of partitions*, Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976. xiv+255 pp.
- [4] P. Aubry, *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom*, Thèse doctorat, Université P. et M. Curie, Paris, janvier 1999.
- [5] P. Aubry, D. Lazard, M. Moreno, *On the theories of triangular sets*, J. of Symbolic Computation, Special Issue on Polynomial Elimination, 28(1), 1999, p. 105-124.
- [6] W. Auzinger, W. and H. J. Stetter, *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, In Proc. Intern. Conf. on Numerical Math., vol. 86 of Int. Series of Numerical Math, Birkhuser Verlag, 1988, p. 12-30.
- [7] A. Ayad, *Complexity bound of absolute factoring of parametric polynomials*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 316, Teor. Slozhn. Vychisl. 9, 224 (2004), p. 5-29.
- [8] S. Basu, R. Pollack, M-F. Roy, *Algorithms in real algebraic geometry*, Springer, New York, 2003.
- [9] M. Ben-Or, D. Kozen, and J. Reif, *The complexity of elementary algebra and geometry*, Journal of Computer and System Sciences 32, 251-264, 1986.
- [10] E.R. Berlekamp, *Factoring polynomials over finite fields*, Bell Systems Tech. J., 46, 1967, p. 1853-1859.
- [11] E.R. Berlekamp, *Factoring polynomials over large finite fields*, Math.Comp., 24, 1970, p. 713-735.
- [12] A. Bostan, G. Lecerf, B. Salvy, É. Schost, B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, ISSAC 2004, Spain, p. 42 - 49.

- [13] B. Buchberger, *Gröbner Bases : An algorithmic method in polynomial ideal theory*, in Multidimensional System Theory (N.K.Bose et al.,Eds), Reidel, Dordrecht, 1985, p. 374-383.
- [14] B. Buchberger, G. E. Collins, R. Loos, R. Albrecht, *Computer Algebra : Symbolic and Algebraic Computation*, Wien, Springer, 1983.
- [15] P. Burgisser, M. Clausen, M.A. Shokrollahi, *Algebraic Complexity Theory*, Springer 1997.
- [16] J. Canny, D. Grigoriev, N. Vorobjov, *Finding connected components of a semialgebraic set in subexponential time*, Appl. Algebra Engrg. Comm. Comput. 2 (1992), No. 4, p. 217-238.
- [17] J. F. Canny, E. Kaltofen, Y.N. Lakshman, *Solving Systems of Nonlinear Polynomial Equations Faster*, ISSAC 1989, p. 121-128.
- [18] J. F. Canny, *Generalised Characteristic Polynomials*, J. Symb. Comput. 9(3), 1990, p. 241-250.
- [19] G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*, Thèse doctorat, Université de Nice - Sophia-Antipolis, 2004.
- [20] G. Chèze, G. Lecerf, *Lifting and recombination techniques for absolute factorization*, Manuscript, Université de Versailles Saint-Quentin-en-Yvelines, 2005.
- [21] G. Chèze, A. Galligo, *From an approximate to an exact factorization*, Prépublication de l'Université de Nice, 2003.
- [22] A.L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math., 34(1986), No. 4 p. 1838-1882.
- [23] A.L. Chistov, D. Grigoriev, *Subexponential-time solving systems of algebraic equations*, I and II, LOMI Preprint, Leningrad, 1983, E-9-83, E-10-83.
- [24] A. Chistov, D. Grigoriev, *Complexity of quantifier elimination in the theory of algebraically closed fields*, LNCS, vol. 176 (1984), p. 17-31.
- [25] A. Chistov, D. Grigoriev, *Polynomial-time factoring of the multivariable polynomials over a global field*, Preprint LOMI E-5-82, Leningrad, 1982.
- [26] A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde Matrices, NP-Completeness, and Transversal Subspaces*, Foundations of Computational Mathematics 3(4), 2003, p. 421-427.
- [27] A. M. Cohen, J. H. Davenport, A. J. P. Heck, *An overview of computer algebra*, In "Computer Algebra in Industry, Problem Solving in Practice", Edited by Arjeh M. Cohen, Wiley, 1991, p. 1-52.
- [28] G.E. Collins, *Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition*, Lect. Notes Comput. Sci. 33, 1975, p. 134-183.

- [29] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*, In proceedings of the Nineteenth Annual ACM Symposium on Theory of computing, 1987, p. 1-6.
- [30] R. M. Corless, A. Galligo, I. S. Kotsireas, S. M. Watt, *A geometric-numeric algorithm for absolute factorization of multivariate polynomials*, ISSAC 2002, France, p. 37 - 45.
- [31] D. Cox, J. Little, D. O'shea, *Ideals, Varieties and Algorithms*, Second Edition, Springer 1997.
- [32] D. Cox, J. Little, D. O'shea, *Using Algebraic Geometry*, Springer, 1998.
- [33] X. Dahan, E. Schost, *Sharp estimates for triangular sets*, Proceedings ISSAC 2004.
- [34] J. Davenport, J. Heintz, *Real quantifier elimination is doubly exponential*, J. of Symbolic Computation, t. 5, 1988, p. 29-35.
- [35] A. Dickenstein, L. Z. Emiris, *Solving Polynomial Equations, Foundations, Algorithms, and Applications*, Springer, 2005.
- [36] M. Elkadi, B. Mourrain, *A new algorithm for the geometric decomposition of a variety*, Proceedings of the 1999 international symposium on Symbolic and algebraic computation, Canada, 1999, p. 9-16.
- [37] M. J. Encarnación, *An Efficient Method for Computing Resultant Systems*, Applicable Algebra in Engineering, Communication and Computing, 1998, 9, 3, p. 243-245.
- [38] J.C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 international symposium on Symbolic and algebraic computation, 2002, Lille, France, p. 75-83.
- [39] J. C. Faugère , P. Gianni , D. Lazard , T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Journal of Symbolic Computation, Vol. 16 N. 4, Oct. 1993, p. 329-344.
- [40] N. Fitchas, A. Galligo, and J. Morgenstern, *Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields*, J. Pure Appl. Algebra 67 (1990), no. 1, p. 1-14.
- [41] K. Gatermann, X. Bincan, *Existence of 3 Positive Solutions of Systems from Chemistry*, July 2003.
- [42] S. Gao, *Factoring multivariate polynomials via partial differential equations*, American Mathematical Society, vol. 72, Issue 242 (2003), p. 801-822.
- [43] S. Gao, E. Kaltofen, J. May, Z. Yang, L. Zhi, *Approximate factorization of multivariate polynomials via differential equations*, ISSAC 2004, Spain, p. 167-174.
- [44] X-S. Gao, S-C. Chou, *Solving parametric algebraic systems*, ISSAC 1992, California USA, p. 335 - 341.
- [45] P. Gianni and B. Trager *Gröbner bases and primary decomposition in polynomial ideals*, Journal of Symbolic Computation, 6, 148-166, 1988.
- [46] P. Gianni, *Properties of Gröbner bases under specializations*, In Davenport, J.H., ed, EURO-CAL'87, LNCS 378, p. 293-297, New York, Springer.

- [47] M. Giusti, E. Schost, *Solving some overdetermined polynomial systems*, Proc. of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), p. 1-8 (electronic), ACM, New York, 1999.
- [48] M. Giusti, J. Heintz, *Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles*, Effective methods in algebraic geometry (Castiglione, 1990), p. 169-194.
- [49] M. Giusti, J. Heintz, K. Hägele, J.E. Morais, L.M. Pardo, J.I. Montana, *Lower bounds for diophantine approximations*, J. of Pure and Applied Algebra, 117 and 118 (1997), p. 277-317.
- [50] M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, in Computational Algebraic Geometry and Commutative Algebra, Symposia Mathematica (D. Eisenbud and L. Robbiano, Eds.), Vol. 34, Cambridge Univ. Press, Cambridge, UK, 1993, p.216-256.
- [51] M. Giusti, J. Heintz, J. E. Morais, L. M. Pardo, *When Polynomial Equation Systems Can Be Solved Fast ?*, Actes de AAEECC'11 (Paris 1995), Lecture Notes in Computer Science, Vol. 948, Springer Verlag, p. 205 - 231.
- [52] M. Giusti, G. Lecerf, B. Salvy, *A Gröbner free alternative for polynomial system solving*, Journal of Complexity, Vol. 17 N. 1, 2001, p. 154-211.
- [53] M.-J. Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso, A. Zanzi, *Gröbner bases specialization through Hilbert functions : the homogeneous case*, ACM SIGSAM Bulletin, Volume 34 , Issue 1, (March 2000), p. 1-8.
- [54] M.-J. Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso, A. Zanzi, *Parametric*, Report Research, The FRISCO Consortium, 2000.
- [55] M.-J. Gonzalez-Lopez, T. Recio, *The ROMIN inverse geometric model and the dynamic evaluation method*, In "Computer Algebra in Industry, Problem Solving in Practice", Edited by Arjeh M. Cohen, Wiley, 1991, p. 117- 141.
- [56] H-G. Gräbe, *On Factorized Gröbner Bases*, In "Computer Algebra in Science and Engineering" (ed. Fleischer, Grabmeier, Hehl, Küchlin), World Scientific Singapore, 1995, p. 77-89.
- [57] H-G. Gräbe, *Minimal Primary Decomposition and Factorized Gröbner Bases*, in J. AAEECC, 8 (1997), p. 265-278.
- [58] D. Grigoriev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations*, J. Sov. Math., 34(1986), No.4 p. 1762-1803.
- [59] D. Grigoriev, *Complexity of quantifier elimination in the theory of ordinary differential equations*, Lecture Notes Computer Science, vol. 378 (1989), p. 11-25.
- [60] D. Grigoriev, N. Vorobjov, *Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute*, Proc. ACM Intern. Conf. Symb and Algebraic Computations, Scotland, 2000, p. 137-145.

- [61] D. Grigoriev, *Constructing double-exponential number of vectors of multiplicities of solutions of polynomial systems*, In Contemporary Math., AMS, 2001, vol. 286, p. 115-120.
- [62] D. Grigoriev, N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, J. Symbolic Computation, t. 5, 1988, p. 37-64.
- [63] D. Grigoriev, *Complexity of deciding Tarski algebra*, J. Symbolic Computation, t. 5, 1988, p. 65-108.
- [64] A. Hashemi, D. Lazard, *Sharper Complexity Bounds for Zero-dimensional Gröbner Bases and Polynomial System Solving*, Rapport de recherche, INRIA, February 2005.
- [65] J. Heintz, T. Krick, S. Puddu, J. Sabia and A. Waissbein, *Deformation Techniques for efficient polynomial equation solving*, Journal of Complexity, 16(2000), p. 70-109.
- [66] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. 24, 3 (1983), p. 239-277.
- [67] J. Heintz, G. Matera, A. Waissbein, *On the Time-Space Complexity of Geometric Elimination Procedures*, Appl. Algebra Eng. Commun. Comput. 11(4), 2001, p. 239-296.
- [68] J. Heintz, M-F. Roy, P. Solernó, *Sur la complexité du principe de Tarski-Seidenberg*, Bulletin de la Société Mathématique de France, 118 no. 1 (1990), p. 101-126.
- [69] G. Jeronimo, J. Sabia, *Effective equidimensional decomposition of affine varieties*, J. Pure Appl. Algebra, 169 (2-3) (2002), p. 229-248.
- [70] M. Kalkbrenner, *On the stability of Gröbner bases under specializations*, J. of Symb. Comp., 24, 1997, p. 51-58.
- [71] E. Kaltofen, *On the complexity of factoring polynomials with integer coefficients*, PhD thesis, Rensselaer Polytechnic Instit., Troy, N.Y., December 1982.
- [72] E. Kaltofen, *Factorization of polynomials*, Computer algebra, 95-113, Springer, Vienna, 1983.
- [73] E. Kaltofen and V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, In Proc. 27th Annual ACM Symp. Theory Comput., New York, N.Y., 1995. ACM Press, p. 398-406.
- [74] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization*, SIAM J. Comput., 14(2), 1985, p. 469-489.
- [75] D. Kapur, *An Approach for Solving Systems of Parametric Polynomial Equations*, Principles and Practice of Constraint Programming, (eds. Saraswat and Van Hentenryck), MIT press, 1995.
- [76] T. Krick, L.M. Pardo, *A computational method for diophantine approximation*, Algorithms in algebraic geometry and applications (Santander, 1994), p. 193-253.
- [77] Y. N. Lakshman, *A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals*, Effective methods in algebraic geometry, Progress in Mathematics, 94, Birkhäuser Verlag, Basel, 1991, p. 227-234.

- [78] S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput., 14 (1985), p. 184-195.
- [79] S. Lang, *Algebra*, Addison-Wesley , 1993.
- [80] D. Lazard, *Algèbre linéaire sur $k[X_1, \dots, X_n]$ et élimination*, Bull. Soc. Math. France, 105, 1977, p. 165-190.
- [81] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theo. Comput, Sci, 15, 1981, p. 77-110.
- [82] D. Lazard, *Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations*, EUROCAL 1983, p. 146-156.
- [83] D. Lazard, *On the specification for solvers of polynomial systems*, 5th Asian Symposium on Computers Mathematics -ASCM 2001, Matsuyama, Japan. Lecture Notes Series in Computing, 9, World Scientific, 2001, p. 66-75.
- [84] D. Lazard, F. Rouillier, *Solving parametric polynomial systems*, Rapport de recherche, INRIA, Projet SALSA, Octobre 2004.
- [85] D. Lazard, *Resolution of polynomial systems*, Computers Mathematics. Proceedings of the Fourth Asian Symposium (ASCM 2000). Xiao-Shan Gao, Dongming Wang ed. World Scientific (2000), p. 1-8.
- [86] D. Lazard, *Solving zero-dimensional algebraic systems*, Journal of Symbolic Computation, Vol. 13, 1992, p. 117-131.
- [87] G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 international symposium on Symbolic and algebraic computation symbolic and algebraic computation, St. Andrews, Scotland, July 2000, p. 209-216.
- [88] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, Journal of Complexity, Volume 19 , Issue 4 (August 2003), p. 564-596.
- [89] A.K. Lenstra, H.W.Jr. Lenstra, L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), no.4, 515-534.
- [90] A.K. Lenstra, *Factoring multivariate polynomial over finite fields*, J. Comput. System Sci. 30 (1985), N. 2, p. 235-248.
- [91] A. K. Lenstra, *Factoring multivariate polynomials over algebraic number fields*, SIAM J. Comput. 16 (1987), p. 591-598.
- [92] G. Lyubeznik, *Minimal resultant systems*, Journal of Algebra, 1995, 177, p. 612-616.
- [93] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics. Cambridge University Press, 1916.
- [94] D. Manocha, J. Canny, *Multipolynomial resultant algorithms*, Journal of Symbolic Computation, 15(2), 1993, p. 99-122.

- [95] G. Matera, J.M.T. Torres, *The Space Complexity of Elimination Theory : Upper bounds*, Foundations of Computational Mathematics, FOCM'97, Springer Verlag, 1997, p. 267-276.
- [96] M. Mignotte, D. Stefanescu, *Polynomials An Algorithmic Approach*, Springer 1999.
- [97] M. Mignotte, *Mathématiques pour le calcul formel*, Presses universitaires de France, Paris, 1989.
- [98] B. Mishra, *Algorithmic Algebra*, Springer-Verlag, 1993.
- [99] H.M. Moller, R. Tenberg, *Multivariate polynomial system solving using intersections of eigenspaces*, J. Symbolic Computation (2001), 32, p. 513-531.
- [100] A. Montes, *A new algorithm for discussing Gröbner basis with parameters*, J. of Symb. Comp., 33, 2002, p. 183-208.
- [101] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties*, Springer-Verlag Berlin Heidelberg New York 1995.
- [102] D.R. Musser, *Multivariate polynomial factorization*, J. of A.C.M. t. 197, 1975, p. 291-309.
- [103] D.R. Musser, *Algorithms for polynomial factorization*, PhD, thesis and TR 134, Univ. of Wisconsin, 1971.
- [104] S. Puddu, J. Sabia, *An effective algorithm for quantifier elimination over algebraically closed fields using straight-line programs*, J. of Pure and Appl. Algebra, 129, 1997, p. 173-200.
- [105] J-F. Ragot , *Sur la factorisation absolue des polynômes*, Thèse à l'université de Limoges, Décembre 1997.
- [106] J. Renegar, *On the Computational Complexity and Geometry of the Firstorder Theory of the Reals : Parts I-III*, Journal of Symbolic Computation, 1992, 13, p. 255- 352.
- [107] K. Rimey, *A System of Polynomial Equations and a Solution by an Unusual Method*, SIGSAM Bulletin, 18(1), February 1984, p. 30-32.
- [108] F. Rouillier, *Solving zero-dimensional polynomial systems through the rational univariate representation*, Tech. Rep. 3426, INRIA, Projet Polka, 1998.
- [109] E. Schost, *Computing Parametric Geometric Resolutions*, Applicable Algebra in Engineering, Communication and Computing 13(5), 2003, p. 349 - 393.
- [110] E. Schost, *Sur la résolution des systèmes polynomiaux à paramètres*, Thèse de doctorat, École polytechnique, décembre 2000.
- [111] E. Schost, *Complexity results for triangular sets*, Journal of Symbolic Computation 36(3-4), 2003, p. 555-594.
- [112] I.R. Shafarevich, *Basic Algebraic Geometry*, Springer 1974.
- [113] W.Y. Sit, *An algorithm for solving parametric linear systems*, J. Symbolic Computation, 13 (1992), p. 353-394.

- [114] W.Y. Sit, *A theory for parametric linear systems*, Proceedings of the 1991 international symposium on Symbolic and algebraic computation, Bonn, West Germany, 1991, p. 112-121.
- [115] A.J. Sommese, J. Verschelde, and C.W. Wampler, *Numerical decomposition of the solution sets of polynomial systems into irreducible components*, SIAM Journal on Numerical Analysis 38, 2001, p. 2022–2046.
- [116] A. J. Sommese, J. Verschelde, C.W. Wampler, *Numerical factorization of multivariate complex polynomials*, Theoretical Comput. Sci. 315, 2-3 (2004), p. 651-669.
- [117] B.L. Van Der Waerden, *Modern algebra*, Vol 2, 1950.
- [118] J. von zur Gathen, J. Gerhard, *Modern Computer algebra*, Cambridge University Press 1999.
- [119] J. von zur Gathen, E. Kaltofen, *Factorization of multivariate polynomials over finite fields*, Math. Comp. 45 (1985), no.171, p. 251-261.
- [120] D. Wang, *Elimination Practice Software Tools and Applications*, World Scientific Pub Co Inc, 2004.
- [121] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Computation, 14 (1991), p. 1-29.
- [122] V. Weispfenning, *Solving parametric polynomial equations and inequalities by symbolic algorithms*, MIP-9504, Universitat Passau, Januar 1995, in Proc. of the workshop "Computer Algebra in Science and Engineering", Bielefeld, August 1994, World Scientific, 1995, p. 163-179.
- [123] V. Weispfenning, *Quantifier Elimination for Real Algebra - the Cubic Case*, ISSAC, 1994, p. 258-263.
- [124] L. Yang, *Recent Advances on Determining the Number of Real Roots of Parametric Polynomials*, J. Symb. Comput. 28(1-2), 1999, p. 225-242.
- [125] O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1 (Springer-Verlag 1958) and vol. 2 (Springer-Verlag 1976).
- [126] H. Zassenhaus, *On Hensel factorization*, J. Number Theory, 1, 1969, p. 291-311.